INTERNATIONAL TELECOMMUNICATION UNION

# CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

**BLUE BOOK**

---

**VOLUME VI – FASCICLE VI.7**

# SPECIFICATIONS OF SIGNALLING SYSTEM No. 7

**RECOMMENDATIONS Q.700-Q.716**

---

**IXTH PLENARY ASSEMBLY**
MELBOURNE, 14-25 NOVEMBER 1988

Geneva 1989

INTERNATIONAL TELECOMMUNICATION UNION

# CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

**BLUE BOOK**

---

**VOLUME VI – FASCICLE VI.7**

# SPECIFICATIONS OF SIGNALLING SYSTEM No. 7

**RECOMMENDATIONS Q.700-Q.716**

---

**IXTH PLENARY ASSEMBLY**
MELBOURNE, 14-25 NOVEMBER 1988

Geneva 1989

ISBN 92-61-03511-6

Printed in France

## CONTENTS OF THE CCITT BOOK APPLICABLE AFTER THE NINTH PLENARY ASSEMBLY (1988)

## BLUE BOOK

FASCICLE III.6 – Line transmission of non-telephone signals. Transmission of sound-programme and television signals. Series H and J Recommendations (Study Group XV).

FASCICLE III.7 – Integrated Services Digital Network (ISDN) – General structure and service capabilities. Recommendations I.110-I.257 (Study Group XVIII).

FASCICLE III.8 – Integrated Services Digital Network (ISDN) – Overall network aspects and functions, ISDN user-network interfaces. Recommendations I.310-I.470 (Study Group XVIII).

FASCICLE III.9 – Integrated Services Digital Network (ISDN) – Internetwork interfaces and maintenance principles. Recommendations I.500-I.605 (Study Group XVIII).

**Volume IV**

FASCICLE IV.1 – General maintenance principles: maintenance of international transmission systems and telephone circuits. Recommendations M.10-M.782 (Study Group IV).

FASCICLE IV.2 – Maintenance of international telegraph, phototelegraph and leased circuits. Maintenance of the international public telephone network. Maintenance of maritime satellite and data transmission systems. Recommendations M.800-M.1375 (Study Group IV).

FASCICLE IV.3 – Maintenance of international sound-programme and television transmission circuits. Series N Recommendations (Study Group IV).

FASCICLE IV.4 – Specifications for measuring equipment. Series O Recommendations (Study Group IV).

**Volume V** – Telephone transmission quality. Series P Recommendations (Study Group XII).

**Volume VI**

FASCICLE VI.1 – General Recommendations on telephone switching and signalling. Functions and information flows for services in the ISDN. Supplements. Recommendations Q.1-Q.118 *bis* (Study Group XI).

FASCICLE VI.2 – Specifications of Signalling Systems Nos. 4 and 5. Recommendations Q.120-Q.180 (Study Group XI).

FASCICLE VI.3 – Specifications of Signalling System No. 6. Recommendations Q.251-Q.300 (Study Group XI).

FASCICLE VI.4 – Specifications of Signalling Systems R1 and R2. Recommendations Q.310-Q.490 (Study Group XI).

FASCICLE VI.5 – Digital local, transit, combined and international exchanges in integrated digital networks and mixed analogue-digital networks. Supplements. Recommendations Q.500-Q.554 (Study Group XI).

FASCICLE VI.6 – Interworking of signalling systems. Recommendations Q.601-Q.699 (Study Group XI).

FASCICLE VI.7 – Specifications of Signalling System No. 7. Recommendations Q.700-Q.716 (Study Group XI).

FASCICLE VI.8 – Specifications of Signalling System No. 7. Recommendations Q.721-Q.766 (Study Group XI).

FASCICLE VI.9 – Specifications of Signalling System No. 7. Recommendations Q.771-Q.795 (Study Group XI).

FASCICLE VI.10 – Digital subscriber signalling system No. 1 (DSS 1), data link layer. Recommendations Q.920-Q.921 (Study Group XI).

FASCICLE VI.11 – Digital subscriber signalling system No. 1 (DSS 1), network layer, user-network management. Recommendations Q.930-Q.940 (Study Group XI).

FASCICLE VI.12 – Public land mobile network. Interworking with ISDN and PSTN. Recommendations Q.1000-Q.1032 (Study Group XI).

FASCICLE VI.13 – Public land mobile network. Mobile application part and interfaces. Recommendations Q.1051-Q.1063 (Study Group XI).

FASCICLE VI.14 – Interworking with satellite mobile systems. Recommendations Q.1100-Q.1152 (Study Group XI).

**Volume VII**

FASCICLE VII.1 – Telegraph transmission. Series R Recommendations. Telegraph services terminal equipment. Series S Recommendations (Study Group IX).

FASCICLE VII.2 – Telegraph switching. Series U Recommendations (Study Group IX).

FASCICLE VII.3 – Terminal equipment and protocols for telematic services. Recommendations T.0-T.63 (Study Group VIII).

FASCICLE VII.4 – Conformance testing procedures for the Teletex Recommendations. Recommendation T.64 (Study Group VIII).

FASCICLE VII.5 – Terminal equipment and protocols for telematic services. Recommendations T.65-T.101, T.150-T.390 (Study Group VIII).

FASCICLE VII.6 – Terminal equipment and protocols for telematic services. Recommendations T.400-T.418 (Study Group VIII).

FASCICLE VII.7 – Terminal equipment and protocols for telematic services. Recommendations T.431-T.564 (Study Group VIII).

**Volume VIII**

FASCICLE VIII.1 – Data communication over the telephone network. Series V Recommendations (Study Group XVII).

FASCICLE VIII.2 – Data communication networks: services and facilities, interfaces. Recommendations X.1-X.32 (Study Group VII).

FASCICLE VIII.3 – Data communication networks: transmission, signalling and switching, network aspects, maintenance and administrative arrangements. Recommendations X.40-X.181 (Study Group VII).

FASCICLE VIII.4 – Data communication networks: Open Systems Interconnection (OSI) – Model and notation, service definition. Recommendations X.200-X.219 (Study Group VII).

FASCICLE VIII.5 – Data communication networks: Open Systems Interconnection (OSI) – Protocol specifications, conformance testing. Recommendations X.220-X.290 (Study Group VII).

FASCICLE VIII.6 – Data communication networks: interworking between networks, mobile data transmission systems, internetwork management. Recommendations X.300-X.370 (Study Group VII).

FASCICLE VIII.7 – Data communication networks: message handling systems. Recommendations X.400-X.420 (Study Group VII).

FASCICLE VIII.8 – Data communication networks: directory. Recommendations X.500-X.521 (Study Group VII).

**Volume IX** – Protection against interference. Series K Recommendations (Study Group V). Construction, installation and protection of cable and other elements of outside plant. Series L Recommendations (Study Group VI).

**Volume X**

FASCICLE X.1 – Functional Specification and Description Language (SDL). Criteria for using Formal Description Techniques (FDTs). Recommendation Z.100 and Annexes A, B, C and E, Recommendation Z.110 (Study Group X).

FASCICLE X.2 – Annex D to Recommendation Z.100: SDL user guidelines (Study Group X).

FASCICLE X.3 – Annex F.1 to Recommendation Z.100: SDL formal definition. Introduction (Study Group X).

FASCICLE X.4 – Annex F.2 to Recommendation Z.100: SDL formal definition. Static semantics (Study Group X).

FASCICLE X.5 – Annex F.3 to Recommendation Z.100: SDL formal definition. Dynamic semantics (Study Group X).

FASCICLE X.6 – CCITT High Level Language (CHILL). Recommendation Z.200 (Study Group X).

FASCICLE X.7 – Man-Machine Language (MML). Recommendations Z.301-Z.341 (Study Group X).

## CONTENTS OF FASCICLE VI.7 OF THE BLUE BOOK

**Recommendations Q.700 to Q.716**

**Specifications of Signalling System No. 7**

## REMARKS

1 The strict observance of the specifications for standardized international signalling and switching equipment is of the utmost importance in the manufacture and operation of the equipment. Hence these specifications are obligatory except where it is explicitly stipulated to the contrary.

The values given in Fascicles VI.1 to VI.14 are imperative and must be met under normal service conditions.

2 The Questions entrusted to each Study Group for the Study Period 1989-1992 can be found in Contribution No. 1 to that Study Group.

---

## CCITT NOTE

In this Volume, the expression "Administration" is used for shortness to indicate both a telecommunication Administration and a recognized private operating agency.

FASCICLE VI.7

**Recommendations Q.700 to Q.716**

# SPECIFICATIONS OF SIGNALLING SYSTEM No. 7

PAGE INTENTIONALLY LEFT BLANK

PAGE LAISSEE EN BLANC INTENTIONNELLEMENT

SECTION 1

# GENERAL

## Recommendation Q.700

### INTRODUCTION TO CCITT SIGNALLING SYSTEM No. 7

### 1 General

This Recommendation provides an overview of the Signalling System by describing the various functional elements of CCITT No. 7 and the relationship between these functional elements. This Recommendation provides a general description of functions and capabilities of the Message Transfer Part (MTP), Signalling Connection Control Part (SCCP), Telephone User Part, ISDN User Part (ISDN-UP), Transaction Capabilities (TC), and the Operations, Maintenance and Administration Part (OMAP) which are covered elsewhere in the Q.700 to Q.795 series of Recommendations. However, in the case of contradiction between the specifications and Q.700, the Q.700 to Q.795 specification shall apply.

Supplementary Services in CCITT S.S. No.7 ISDN applications are described in the Q.73x series of Recommendations.

In addition to these functions in the CCITT No. 7 signalling system, the Q.700 to Q.795 series of Recommendations describes the CCITT No. 7 network structure, and also specifies the Tests and Measurements applicable to CCITT No. 7.

This Recommendation is also a specification of those aspects such as CCITT S.S. No. 7 Architecture, Flow Control and general compatibility rule which are not specified in separate Recommendations, and are applicable to the overall scope of S.S. No. 7.

The remainder of this Recommendation describes:

- § 2: Signalling network concepts components and modes;
- § 3: The functional blocks within CCITT Signalling System No. 7 and the services provided by them;
- § 4: CCITT Signalling System No. 7 protocol layering and its relationship to OSI modelling;
- § 5: Node, application entity and user part addressing;
- § 6: Operations, administration and maintenance aspects of CCITT S.S. No. 7;
- § 7: Performance aspects of the functional blocks within CCITT S.S. No. 7;
- § 8: Flow control for both the signalling network and within nodes;
- § 9: Rules for evolving CCITT S.S. No. 7 protocols while preserving compatibility with earlier versions;
- § 10: A cross-reference to a glossary of terms.

#### 1.1 *Objectives and fields of application*

The overall objective of Signalling System No. 7 is to provide an internationally standardised general purpose common channel signalling (CCS) system:

- optimised for operation in digital telecommunications networks in conjunction with stored program controlled exchanges;
- that can meet present and future requirements of information transfer for inter-processor transactions within telecommunications networks for call control, remote control, and management and maintenance signalling;
- that provides a reliable means for transfer of information in correct sequence and without loss or duplication.

The signalling system meets requirements of call control signalling for telecommunication services such as the telephone, ISDN and circuit switched data transmission services. It can also be used as a reliable transport system for other types of information transfer between exchanges and specialised centres in telecommunications networks (e.g. for management and maintenance purposes). The system is thus applicable for multipurpose uses in networks that are dedicated for particular services and in multiservices networks. The signalling system is intended to be be applicable in international and national networks.

The scope of CCITT S.S. No. 7 encompasses both circuit related and non-circuit related signalling.

Examples of applications supported by CCITT S.S. No. 7 are:

- PSTN,
- ISDN,
- Interaction with Network Databases, Service Control Points for service control,
- Mobiles (Public Land Mobile Network),
- Operations Administration and Maintenance of Networks.

The signalling system is optimized for operation over 64-kbit/s digital channels. It is also suitable for operation over analogue channels and at lower speeds. The system is suitable for use on point-to-point terrestrial and satellite links. It does not include the special features required for use in point-to-multipoint operation but can, if required, be extended to cover such an application.

## 1.2 *General characteristics*

Common channel signalling is a signalling method in which a single channel conveys, by means of labelled messages, signalling information relating to, for example, a multiplicity of circuits, or other information such as that used for network management. Common channel signalling can be regarded as a form of data communication that is specialised for various types of signalling and information transfer between processors in telecommunications networks.

The signalling system uses signalling links for transfer of signalling messages between exchanges or other nodes in the telecommunication network served by the system. Arrangements are provided to ensure reliable transfer of signalling information in the presence of transmission disturbances or network failures. These include error detection and correction on each signalling link. The system is normally applied with redundancy of signalling links and it includes functions for automatic diversion of signalling traffic to alternative paths in case of link failures. The capacity and reliability for signalling may thus be dimensioned by provision of a multiplicity of signalling links according to the requirements of each application.

## 1.3 *Components of CCITT S.S. No. 7*

CCITT S.S. No. 7 consists of a number of components or functions which are defined as a series of Q.700 to Q.795 Recommendations.

| *CCITT S.S. No. 7 function* | *Recommendations* |
|---|---|
| Message Transfer Part (MTP) | Q.701-Q.704, Q.706, Q.707 |
| Telephone User Part (TUP) (including supplementary services) | Q.721-Q.725 |
| Supplementary services | Q.730 |
| Data User Part (DUP) | Q.741 (note 1) |
| ISDN User Part (ISDN-UP) | Q.761-Q.764, Q.766 |
| Signalling Connection Control Part (SCCP) | Q.711-Q.714, Q.716 |
| Transaction Capabilities (TC) | Q.771-Q.775 |
| Operations Maintenance and Administration Part (OMAP) | Q.795 |

*Note 1* – Functions of the DUP are fully specified in Recommendation X.61.

Other Q.700 to Q.795 series Recommendations which describe other aspects of the signalling system but not part of the CCITT S.S. No. 7 signalling interfaces are:

| *Title* | *Recommendations* |
|---|---|
| Signalling Network Structure | Q.705 |
| Numbering of International Signalling Point Codes | Q.708 |
| Hypothetical signalling reference connection | Q.709 |
| PABX application | Q.710 |
| CCITT S.S. No. 7 Test Specification (General) | Q.780 |
| MTP Level 2 Test Specification | Q.781 |
| MTP Level 3 Test Specification | Q.782 |
| TUP Test Specification | Q.783 |
| Monitoring and measurements for the CCITT S.S. No.7 network | Q.791 |

§ 3 of Q.700 describes the relationship between these components.

### 1.4 *Description techniques in the Q.700 to Q.795 series of Recommendations*

The CCITT S.S. No. 7 Recommendation series define the signalling system using prose description which is complemented by SDL diagrams and state transition diagrams. Should any conflict arise between the text and the SDL definition, the textual description is taken as definitive.

Message sequence charts or arrow diagrams are used to illustrate examples of signalling procedures, but are not considered definitive.

## 2 CCITT S.S. No. 7 signalling network

### 2.1 *Basic concepts*

A telecommunications network served by common channel signalling is composed of a number of switching and processing nodes inter-connected by transmission links. To communicate using CCITT No. 7, each of these nodes requires to implement the necessary "within node" features of CCITT S.S. No. 7 making that node a signalling point within the CCITT S.S. No. 7 network. In addition, there will be a need to interconnect these signalling points such that CCITT S.S. No. 7 signalling information (data) may be conveyed between them. These data links are the signalling links of CCITT S.S. No. 7 signalling network.

The combination of signalling points and their interconnecting signalling links form the CCITT S.S. No. 7 signalling network.

### 2.2 *Signalling network components*

#### 2.2.1 *Signalling points*

In specific cases there may be a need to partition the common channel signalling functions at such a (physical) node into logically separate entities from a signalling network point of view; i.e., a given (physical) node may be defined as more than one signalling point. One example is an exchange at the boundary between international and national signalling networks.

Any two signalling points, for which the possibility of communication between their corresponding User Part function exists, are said to have a signalling relation.

The corresponding concept for a given User Part is called a user signalling relation.

An example is when two telephone exchanges are directly connected by a bundle of speech circuits. The exchange of telephone signalling relating to these circuits then constitutes a user signalling relation between the Telephone User Part functions in those exchanges in their role as signalling points.

Another example is when administration of customer and routing data in a telephone exchange is remotely controlled from an operation and maintenance centre by means of communication through a common channel signalling system.

Examples of nodes in a signalling network that constitutes signalling points are:

- exchanges (switching centres),
- operation, administration and maintenance centres,
- service control points,
- signalling transfer points.

All signalling points in a CCITT S.S. No. 7 network are identified by a unique code known as a point code (Recommendation Q.704 refers).

### 2.2.2 *Signalling links*

The common channel signalling system uses signalling links to convey the signalling messages between two signalling points. A number of signalling links that directly interconnect two signalling points which are used as a module constitute a signalling link-set. Although a link set typically includes all parallel signalling links, it is possible to use more than one link set in parallel between two signalling points. A group of links within a link set that have identical characteristics (e.g., the same data link bearer rate) is called a link group.

Two signalling points that are directly interconnected by a signalling link are, from a signalling network structure point of view, referred to as adjacent signalling points. Correspondingly, two signalling points that are not directly interconnected are non-adjacent signalling points.

### 2.2.3 *Signalling modes*

The term "signalling mode" refers to the association between the path taken by a signalling message and the signalling relation to which the message refers.

In the associated mode of signalling, the messages relating to a particular signalling relation between two adjacent points are conveyed over a link set, directly interconnecting those signalling points.

In the non-associated mode of signalling, the messages relating to a particular signalling relation are conveyed over two or more linksets in tandem passing through one or more signalling points other than those which are the origin and the destination of the messages.

The quasi-associated mode of signalling is a limited case of the non-associated mode where the path taken by the message through the signalling network is pre-determined and, at a given point in time, fixed.

Signalling System No. 7 is specified for use in the associated and quasi-associated modes. The Message Transfer Part does not include features to avoid out-of-sequence arrival of messages or other problems that would typically arise in a fully non-associated mode of signalling with dynamic message routing.

Examples of signalling modes are illustrated in Figure 1/Q.700.

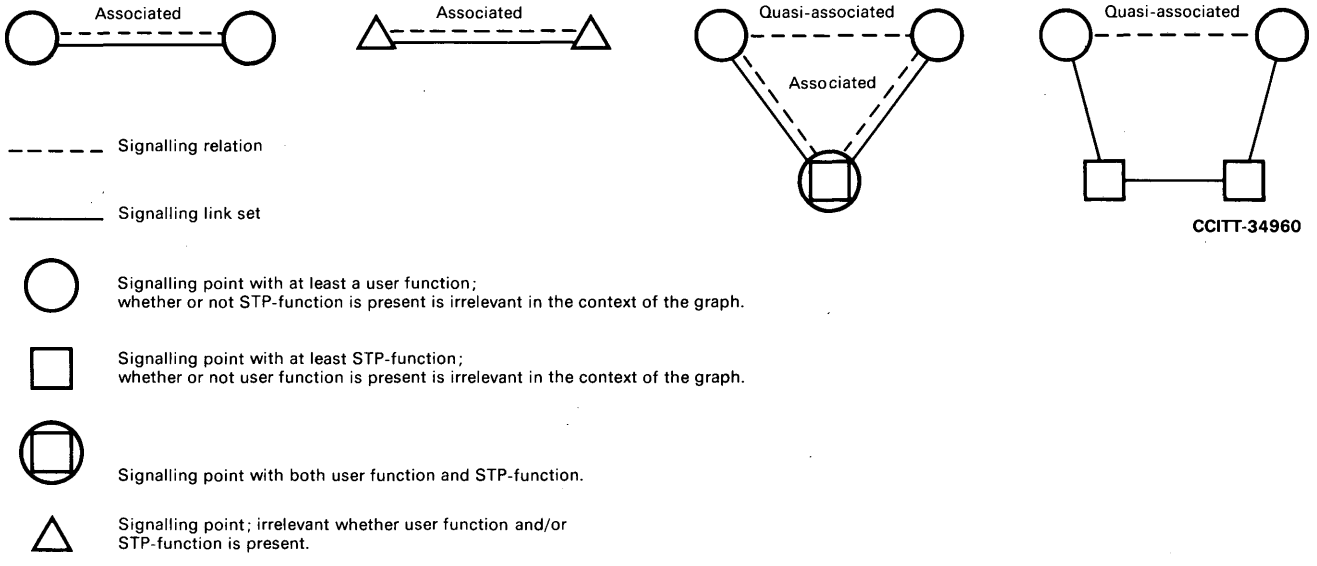



FIGURE 1/Q.700

**Examples of associated and quasi-associated signalling modes and definition of signalling network graph symbols**

2.3 *Signalling point modes*

A signalling point at which a message is generated, i.e., the location of the source User Part function, is the originating point of that message.

A signalling point to which a message is destined, i.e., the location of the receiving User Part function, is the destination point of that message.

A signalling point at which a message is received on a signalling link is transferred to another link, i.e., neither the location of the source nor the receiving User part function, is a Signal Transfer Point (STP).

For a particular signalling relation, the two signalling points thus function as originating and destination points for the messages exchanged in the two directions between them.

In the quasi-associated mode, the function of a signalling transfer point is typically located in a few signalling points which may be dedicated to this function, or may combine this function with some other (e.g., switching) function. A signalling point serving as a signalling transfer point functions as an originating and destination point for the messages generated and received by the level 3 function of the Message Transfer Point also in cases when no user functions are present.

2.4 *Signalling routes*

The pre-determined path, consisting of a succession of signalling points/signalling transfer points and the interconnecting signalling links, that a message takes through the signalling network between the origination point and the destination point is the signalling route for that signalling relation.

All the signalling routes that may be used between an originating point and a destination point by a message traversing the signalling network is the signalling route set for that signalling relation.

2.5 *Signalling network structure*

The signalling system may be used with different types of signalling network structures. The choice between different types of signalling network structures may be influenced by factors such as the structure of the telecommunication network to be served by the signalling system and administrative aspects.

In the case when the provision of the signalling system is planned purely on a per signalling relation basis, the likely result is a signalling network largely based on associated signalling, typically supplemented by a limited degree of quasi-associated signalling for low volume signalling relations. The structure of such a signalling network is mainly determined by the patterns of the signalling relations.

Another approach is to consider the signalling network as a common resource that should be planned according to the total needs for common channel signalling. The high capacity of digital signalling links in combination with the needs for redundancy for reliability then typically leads to a signalling network based on a high degree of quasi-associated signalling with some provision for associated signalling for high volume signalling relations. The latter approach to signalling network planning is more likely to allow exploitation of the potential of common channel signalling to support network features that require communication for purposes other than the switching of connections.

The worldwide signalling network is structured into two functionally independent levels, namely the international and national levels. This structure makes possible a clear division of responsibility for signalling network management and allows numbering plans of signalling points of the international network and the different national networks to be independent of one another.

Further considerations about the structure of the signalling network are given in Recommendation Q.705, and the impact on the message transfer part in Recommendation Q.701.

## 3 CCITT S.S. No. 7 functional blocks

3.1 *Basic functional division*

The Blue Book CCITT Signalling System No. 7 comprises the following functional blocks:

- Message Transfer Part (MTP)
- Telephone User Part (TUP)
- ISDN User Part (ISDN-UP)

- Signalling Connection Control Part (SCCP)
- Transaction Capabilities (TC)
- Application-Entity (AE) *Note 1*
- Application-Service-Elements (ASEs) *Note 1*

*Note 1* – The glossary shows these as hyphenated terms but the usual convention used in this Recommendation will be unhyphenated.

The fundamental principle of the signalling system structure is the division of functions into a common Message Transfer Part (MTP) on one hand, and separate User Parts for different users on the other. This is illustrated in Figure 2/Q.700.

The overall function of the Message Transfer Part is to serve as a transport system providing reliable transfer of signalling messages between the locations of communicating user functions.

User functions in CCITT S.S. No. 7 MTP terms are:

- the ISDN User Part (ISDN-UP)
- the Telephone User Part (TUP)
- the Signalling Connection Control Part (SCCP)
- the Data User Part (DUP)

The term "User" in this context refers to any functional entity that utilises the transport capability provided by the Message Transfer Part.

A User Part comprises those functions of, or related to, a particular type of user that are part of the common channel signalling system, typically because those functions need to be specified in a signalling context.

The SCCP also has Users. These are:

- the ISDN User Part (ISDN-UP)
- Transaction Capabilities (TC)

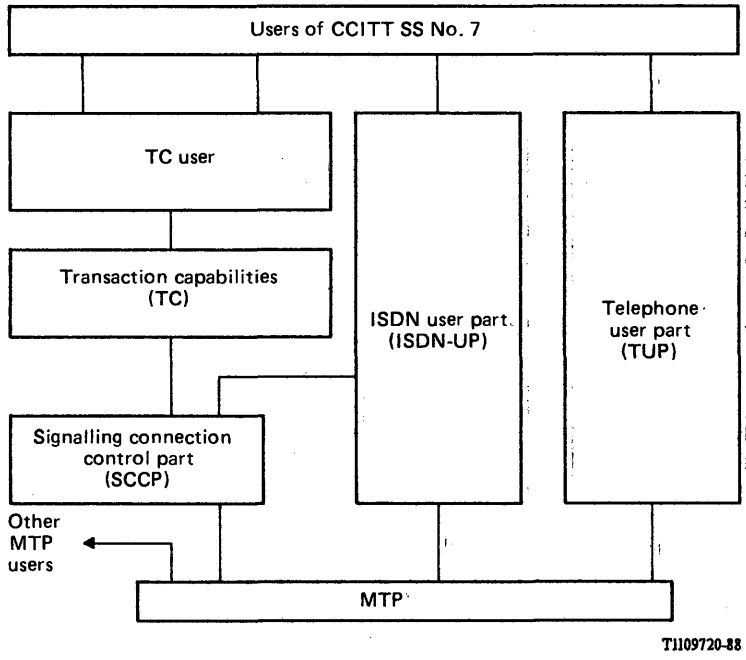



FIGURE 2/Q.700

**Architecture of CCITT SS No. 7**

## 3.2 *CCITT S.S. No. 7 architecture*

### 3.2.1 *General*

Figure 2/Q.700 shows the Architecture of CCITT S.S. No. 7 and illustrates the functional relationship between the various functional blocks of the Blue Book CCITT S.S. No. 7. Figure 5/Q.700 shows the relationship between CCITT No. 7 levels and the OSI Reference Model Layers. This level/layer relationship is described in the following sections.

The initial specification of CCITT No. 7 was based on circuit-related telephony control requirements. To meet these requirements, CCITT No. 7 was specified in four functional levels, the Message Transfer Part comprising levels 1-3, and the User Parts as level 4.

Figure 3/Q.700 shows the Functional Levels of CCITT S.S. No. 7. As new requirements have emerged, e.g., for non-circuit related information transfer, CCITT S.S. No. 7 has also evolved to meet these new requirements. There has been a need to align certain elements in CCITT No. 7 to the OSI 7 Layer Reference Model.

The result of this evolution is that Functional Levels and OSI layers co-exist in CCITT No. 7. For example, the SCCP is a level 4 User Part in MTP terms, but also provides an OSI Network layer 3 service. Subsequent sections describe the various functional elements of CCITT S.S. No. 7 in terms of levels and layers.

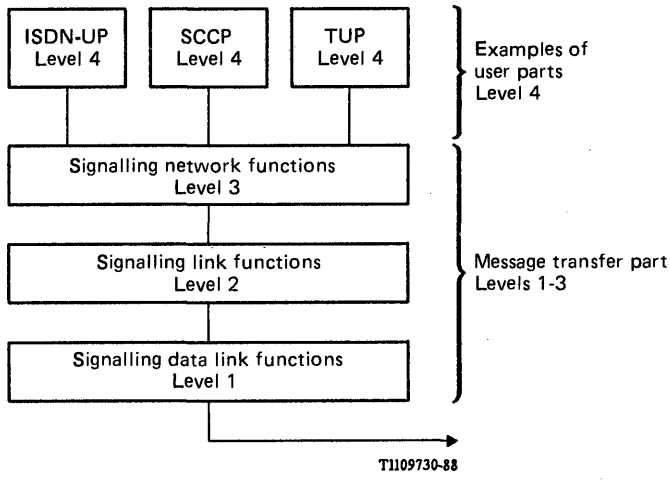



FIGURE 3/Q.700

**CCITT No. 7 functional levels**

It should be noted that the approach proposed for ISDN architecture is to define two orthogonal planes, User and Control, each of which has its own 7-layer protocol reference model.

From the perspective of an end user, the service provided by a telecommunications network may be regarded as a Network Layer Service (User Plane).

Within the telecommunications network, the techniques of the ISDN Protocol Reference Model are applied, and the 7-layer protocol structure of the OSI Model can also be used for inter-nodal communication to the end user.

### 3.2.2 *Message Transfer Part (MTP) levels 1-3*

An overview of the MTP is given in Recommendation Q.701. The MTP is defined in Recommendations Q.701-Q.704, Q.706 and Q.707.

3.2.2.1 *Signalling data link functions (level 1)*

Level 1 defines the physical, electrical and functional characteristics of a signalling data link and the means to access it. The level 1 element provides a bearer for a signalling link.

In a digital environment, 64-kbit/s digital paths will normally be used for the signalling data link. The signalling data link may be accessed via a switching function, providing a potential for automatic reconfiguration of signalling links. Other types of data links, such as analogue links with modems, can also be used.

The detailed requirements for signalling data links are specified in Recommendation Q.702.

3.2.2.2 *Signalling link functions (level 2)*

Level 2 defines the functions and procedures for and relating to the transfer of signalling messages over one individual signalling data link. The level 2 functions together with a level 1 signalling data link as a bearer, and provides a signalling link for reliable transfer of signalling messages between two points.

A signalling message delivered by the higher levels is transferred over the signalling link in variable length signal units. For proper operation of the signalling link, the signal unit comprises transfer control information in addition to the information content of the signalling message.

The detailed requirements for signalling functions are given in Recommendation Q.703.

3.2.2.3 *Signalling network functions (level 3)*

Level 3 in principle defines those transport functions and procedures that are common to and independent of the operation of individual signalling links. These functions fall into two major categories:

a) Signalling message handling functions – These are functions that, at the actual transfer of the message, direct the message to the proper signalling link or User Part.

b) Signalling network management functions – These are functions that, on the basis of predetermined data and information about the status of the signalling network, control the current message routing and configuration of the signalling network facilities. In the event of changes in the status, they also control the reconfigurations and other actions to preserve or restore the normal message transfer capability.

The detailed requirements for signalling network functions are given in Recommendation Q.704.

3.2.3 *Level 4: MTP User functions*

Level 4 consists of the different User Parts. Each User Part defines the functions and procedures of the signalling system that are particular to a certain type of user of the system. the following entities are defined as User Parts in CCITT S.S. No. 7.

3.2.3.1 *Signalling Connection Control Part (SCCP)*

The SCCP is defined in Recommendations Q.711-Q.716. This Recommendation series defines the SCCP capabilities, layer interfaces to MTP and SCCP users signalling messages, their encoding and signalling procedures, and cross-office performance. The SCCP provides additional functions to the Message Transfer Part to provide such connectionless and connection-oriented network services to transfer circuit-related, and non-circuit-related signalling information.

The SCCP provides the means to:

– control logical signalling connections in a CCITT No. 7 network;

– Transfer Signalling Data Units across the CCITT No. 7 network with or without the use of logical signalling connections.

SCCP provides a routing function which allows signalling messages to be routed to a signalling point based on, for example, dialled digits. This capability involves a translation function which translates the global title (e.g., dialled digits) into a signalling point code and a subsystem number.

SCCP also provides a management function, which controls the availability of the "subsystems", and broadcasts this information to other nodes in the network which have a need to know the status of the "subsystem".

The combination of the MTP and the SCCP is called "Network Service Part" (NSP). The Network Service Part meets the requirements for layer 3 services as defined in the OSI-Reference Model, CCITT Recommendation X.200.

3.2.3.2 *Telephone User Part (TUP)*

The CCITT S.S. No. 7 Telephone User Part is defined in Recommendations Q.721-725. The TUP Recommendations define the necessary telephone signalling functions for use of S.S. No. 7 for international telephone call control signalling. This Recommendation series defines the telephone signalling messages, their encoding and signalling procedures, and cross-office performance.

Supplementary Services handled by the CCITT S.S. No. 7 TUP applications are described in Recommendation Q.724, § 10. These supplementary services embody TUP signalling messages and procedures.

3.2.3.3 *Data User Part (DUP)*

The Data User Part is defined in Recommendation Q.741, and the functionality fully defined in Recommendation X.61. It defines the protocol to control interexchange circuits used on data calls, and data call facility registration and cancellation.

3.2.3.4 *ISDN User Part (ISDN-UP)*

The ISDN User Part is defined in Recommendations Q.761-Q.764 and Q.766. This Recommendation series defines the ISDN network signalling messages, their encoding and signalling procedures, and cross-office performance. This Recommendation series deals with the basic services only.

The ISDN-UP encompasses signalling functions required to provide switched services and user facilities for voice and non-voice applications in the ISDN.

The ISDN-UP is also suited for application in dedicated telephone and circuit-switched data networks and in analogue, and mixed analogue/digital networks.

The ISDN-UP has an interface to the SCCP (which is also a level 4 User Part) to allow the ISDN-UP to use the SCCP for end-to-end signalling.

Supplementary Services handled by the CCITT S.S. No. 7 ISDN application are described in Recommendation Q.730. These supplementary services embody ISDN-UP signalling messages and procedures. In some cases these services also include application protocol which uses TC and SCCP, as, for example, centralised Closed User Group (CUG).

3.2.3.5 *Transaction Capabilities*

Transaction Capabilities is defined in Recommendations Q.771-Q.775. This Recommendation series defines the Transaction Capabilities signalling messages, their encoding and signalling procedures.

Transaction Capabilities consists of two elements. These are:

- Transaction Capabilities Application Part (TCAP);
- Intermediate Service Part (ISP) [The ISP is for further study (see Note 1, Figure 5/Q.700)].

The TCAP entity is a functional block residing above the ISP in layer 7. TCAP consists of two sub-layers: the Transaction sub-layer, and the Component sub-layer. Further details are given in Recommendation Q.771.

TC, as currently specified, provides services based on a connectionless network service. In this case, no ISP layers 4-6 functions are involved. Connection-oriented TC services, and the layer functions of layers 4-6 are for further study.

TC provides the means to establish non-circuit-related communication between two nodes in the signalling network.

TC provides the means to exchange operations and replies via a dialogue. The X.229 Remote Operations protocol has been extended to provide added functionality in order to accommodate specific user needs. The operations and parameters are part of the Application protocol between TC users.

3.2.3.6 *Application Entities and Application Service Elements*

In an OSI environment, communication between application processes is modelled by communication between "Application Entities (AEs)". An Application Entity represents the communication functions of an Application process. There may be multiple sets of OSI communication functions in an application process, so a single application process may be represented by multiple AEs. However, each Application Entity is a set of communication capabilities whose components are "Application Service Elements". An Application Service Element (ASE) is a coherent set of integrated functions.

3.2.3.6.1 *Application Entities in a CCITT S.S. No. 7 environment*

Figure 4/Q.700 shows the relationship between Application Processes and Application Entities, and Application Service Elements.

An "Application Process" is considered to be a range of functions and features which support a particular network requirement. For example, an application process in the context of CCITT S.S. No. 7 provides the co-ordination across circuit-related protocols where required.

An Application Process can be considered as:

a) a co-ordinator of specific aspects of network operation (e.g., ISDN Call Control, Mobiles, OA&M);

b) an individual service or supplementary service control function (e.g., CUG).

In the CCITT S.S. No. 7 context, the various functional elements of the signalling system provide the signalling protocols (information elements, messages, and procedures) necessary to support the service between nodes.

In a CCITT No. 7 environment, Application Entities (AEs) are the elements representing the communication functions of the application process, which are pertinent to inter-nodal communication using layer 7 application protocols.

The options for the relationship between an application process, AEs and ASEs can take several forms at a CCITT No. 7 signalling point. Some examples are shown in Figure 4/Q.700.

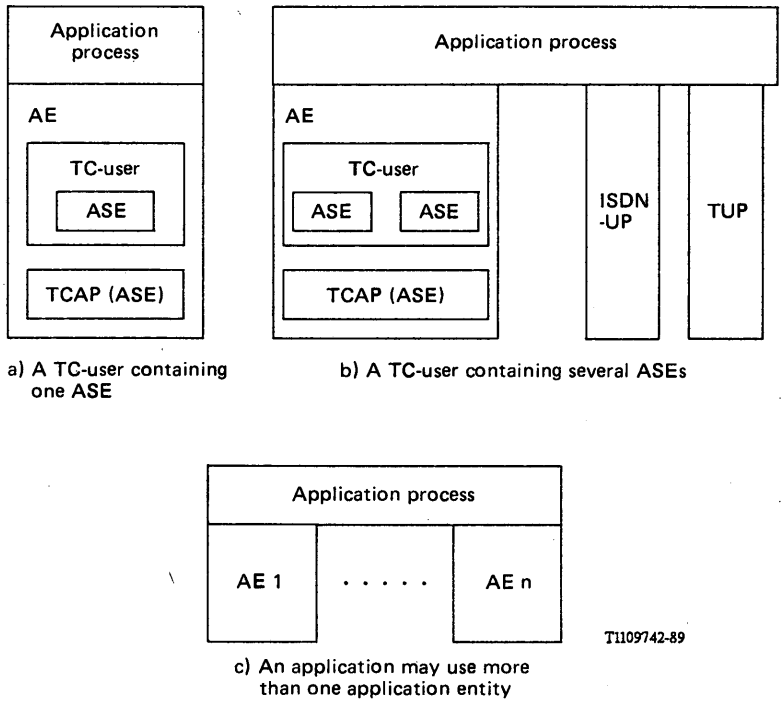



FIGURE 4/Q.700

**Example of the relationship between the application process, AEs and ASEs**

3.2.3.6.2 *Application Service Elements in a CCITT No. 7 environment*

Application Service Elements (ASEs) reside in the CCITT S.S. No. 7 Architecture Model within layer 7 above TCAP. In the context of OSI, TCAP could also be considered to be an ASE.

OMAP has an Application Entity currently containing the TCAP ASE and one other ASE. Other ASEs are under study. OMAP is described further in § 6.

The Mobile Application Part (MAP) is another example of an Application Entity (AE) (see Recommendation Q.1051).

An ASE can include a number of signalling procedures for a single service (e.g., Freephone), where this single service is the application.

Alternatively, an ASE can include a number of signalling procedures for any number of services or functions, encompassed by an application (e.g., MAP, OMAP).

Thus, an ASE can define an individual service protocol (e.g., CUG), or a complete application protocol (e.g., MAP).

An ASE can only communicate with a compatible peer ASE. The operations defined in an ASE may be either symmetrically invoked by each entity involved in the dialogue, or asymmetrically invoked by one entity only (i.e., on a "client/server" basis). An example of the former is a "look ahead if free" procedure; an example of the latter is a database enquiry.

3.2.3.6.3 *Addressing for Application Entities (AEs)*

The SCCP provides a mechanism for addressing "subsystems" using Subsystem Numbers (SSNs). The Application Entity is considered, in the connectionless mode, equivalent to an SCCP subsystem.

3.2.3.6.4 *Management of AEs*

The SCCP provides a mechanism for managing "subsystems" and signalling points and informing other nodes of relevant availability status.

## 4 OSI layering and CCITT S.S. No. 7

### 4.1 *General*

Evolution of the CCITT Signalling System No. 7 architecture has been based on the Open Systems Interconnection (OSI) Reference Model.

The purpose of the Reference Model of Open Systems Interconnection for CCITT Applications (Recommendation X.200) is to provide a well-defined structure for modelling the interconnection and exchange of information between users in a communications system. This approach allows standardised procedures to be defined not only to provide an open systems interconnection between users over a single network, but also to permit interworking between networks to allow communication between users over several networks in tandem.

At present, OSI only considers connection-oriented protocols, that is, protocols which establish a logical connection before transferring data. In CCITT S.S. No. 7, the ISDN-UP uses the SCCP connection-oriented protocol. The CCITT S.S. No. 7 Network Service Part (NSP) provides both connectionless and connection-oriented protocol.

The approach taken in the OSI reference model is to partition the model used to describe this interconnection and exchange information between users in a communications system into seven layers.

From the point of view of a particular layer, the lower layers provide a "transfer service" with specific features. The way in which the lower layers are realised is immaterial to the next higher layers. Correspondingly, the lower layers are not concerned with the meaning of the information coming from higher layers or the reasons for its transfer.

The characteristics of each layer are described below.

4.1.1 *Physical Layer*

The Physical Layer (layer 1) provides transparent transmission of a bit stream over a circuit built in some physical communications medium. It furnishes the interface to the physical media and is responsible for relaying bits (i.e., interconnects data-circuits). A 64 kbit/s link is assumed for the CCITT S.S. No. 7 Physical Layer.

4.1.2 *Data Link Layer*

The Data Link Layer (layer 2) overcomes the limitations inherent in the physical circuits and allows errors in transmission to be detected and recovered, thereby masking deficiencies in transmission quality.

4.1.3 *Network Layer*

The Network Layer (layer 3) transfers data transparently by performing routing and relaying of data between end users. One or more of the sub-networks may interwork at the Network Layer to provide an end user to end user network service. A connectionless network provides for the transfer of data between end users, making no attempt to guarantee a relationship between two or more data messages from the same user.

4.1.4 *Transport Layer*

The Transport Layer (layer 4) provides end user to end user transfer optimising the use of resources (i.e., network service) according to the type and character of the communication, and relieves the user of any concern for the details of transfer. The Transport Layer always operates end-to-end, enhancing the Network Layer when necessary to meet the quality of service objectives of the users.

4.1.5 *Session Layer*

The Session Layer (layer 5) co-ordinates the interaction within each association between communicating application processes. Full and half duplex dialogues are examples of possible Session Layer modes.

4.1.6 *Presentation Layer*

The Presentation Layer (layer 6) transforms the syntax of the data which is to be transferred into a form recognizable by the communicating application processes. For example, the Presentation Layer may convert a data stream from ASCII to EBCDIC.

4.1.7 *Application Layer*

The Application Layer (layer 7) specifies the nature of the communication required to satisfy the users' needs. This is the highest layer in the Model and so does not have a boundary with a higher layer. The Application Layer provides the sole means for the application processes to access the OSI environment.

4.2 *Relationship between CCITT S.S. No. 7 layering and the OSI model*

Layers 1-3 comprise functions for the transportation of information from one location to another, possibly via a number of communication links in tandem. These functions provide the basis on which a communication network can be built.

– The SCCP provides, with the MTP, OSI layer services 1-3.

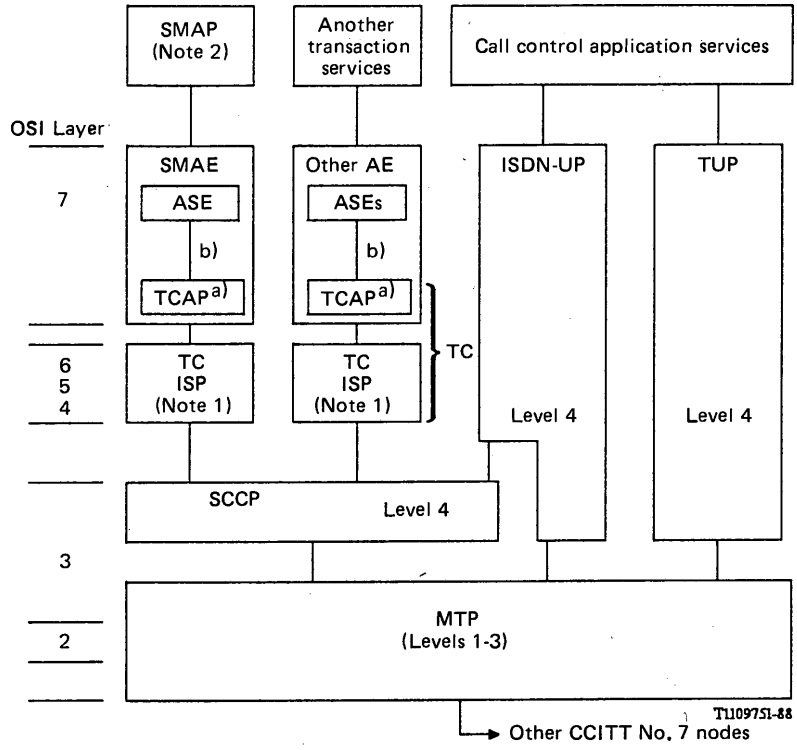
Layers 4-7 define functions relating to end-to-end communication. These layers are so defined that they are independent of the internal structure of the communication network.

– Transaction Capabilities provides layer 4-7 services.

Layer 7 represents the semantics of a communication, whereas layers 1-6 comprise the means by which the communication may be realised.

– Application Entities/Application Service Elements provide the appropriate Application Layer Protocols in layer 7.

Figure 5/Q.700 shows the relationship between SCCP, TC, and ASEs to the OSI 7 Layer Reference Model.




a) TCAP is an ASE.

b) CCITT SS No. 7 primitive interface.

*Note 1* – The TC ISP is for further study. As no signalling procedures are presently specified for this function, the TCAP messages are presented directly to the SCCP. Specific requirements for this ISP function will be defined when needed for future ASEs.

*Note 2* – The set of functions that collectively encompass systems management are known as the Systems Management Application Process (SMAP).

FIGURE 5/Q.700

**Relationship between CCITT No. 7 functional levels and OSI layering**

The aspect of the SMAP which is then involved with communication is the Systems Management Application Entity (SMAE). The SMAE is also known as the OMAP AE.

## 4.3 *Primitive Interfaces between CCITT No. 7 Functions*

### 4.3.1 *General*

Interfaces between the functional elements of CCITT S.S. No. 7 are specified using interface primitives. Primitive interface definition does not assume any specific implementation of a service.

### 4.3.2 *OSI service primitives*

Where the functional element of CCITT No. 7 is modelled on the OSI 7 layer reference model, e.g., SCCP, TC, service primitives are defined in line with Recommendation X.210.

In line with Recommendation X.210, Figure 6/Q.700 illustrates the relationship between the terms "service", "boundary", "service primitives", "peer protocol" and "peer entities". The term "boundary" applies to boundaries between layers, as well as to boundaries between sub-layers.

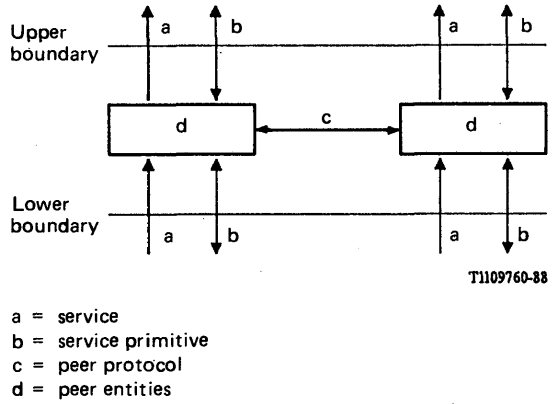



FIGURE 6/Q.700

**Types of service primitives**

4.3.2.1 *Service primitives*

The user of primitives does not preclude any specific implementation of a service in terms of interface primitives.

A service primitive consists of a name and one or more parameters which are passed in the direction of service primitive.

The name of a service primitive contains three elements, as defined in Recommendation X.210:

a) a type indicating the direction of the primitive flow. Four types of service primitives are identified (Figure 7/Q.700):

- request — a primitive issued by a service user to invoke a service element,
- indication — a primitive issued by a service provider to advise that a service element has been invoked by the service user at the peer service access point or by the service provider,
- response — a primitive issued by the service user to complete at a particular service access point some service element whose invocation has been previously indicated at that service access point,
- confirmation — a primitive issued by a service provider to complete at a particular service access point some service element previously invoked by a request at that service access point.

Not all four types can be associated with all service names.

b) a name which specifies the action to be performed;

c) An initial (or initials) which specifies the (sub-)layer providing the service:

- OM for the Operations Management primitives associated with OMAP;
- TC for the TCAP Component sub-layer,
- TR for the TCAP Transaction sub-layer,
- P, S, T, respectively for the Presentation, Session, and Transport layers in the ISP,
- N for the Network Service Part (MTP + SCCP), as defined in Recommendation Q.711.

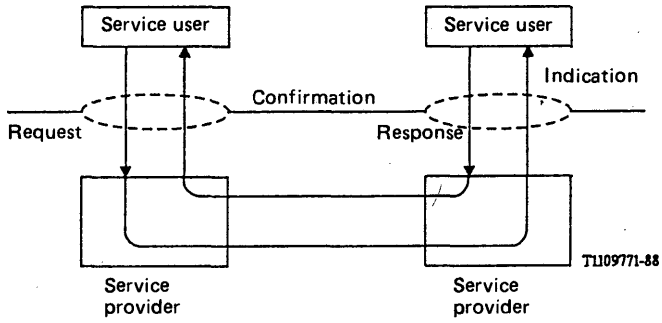



FIGURE 7/Q.700

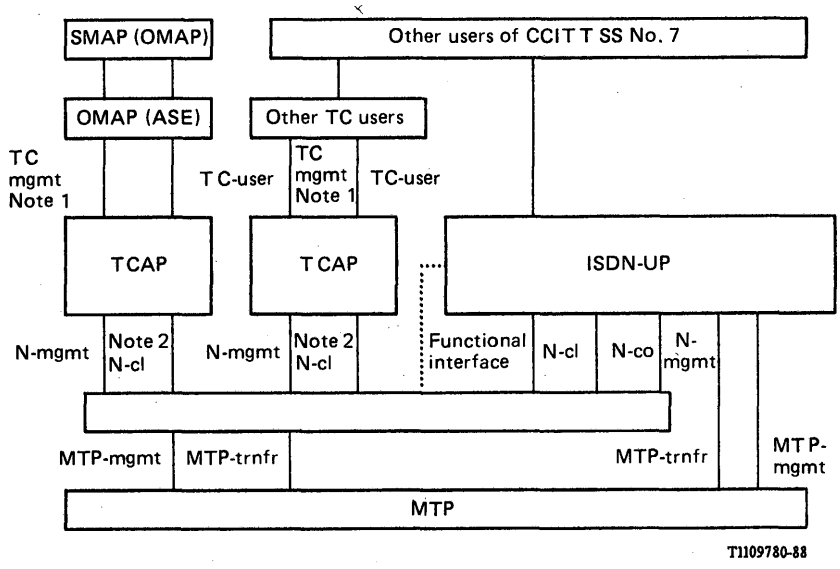
*Types of service primitives*

Figure 8/Q.700 provides an overview of the primitives used between the various functional elements of CCITT No. 7.

The MTP primitives apply to all level 4 users of the MTP.

Similarly, the SCCP Management Primitives N-STATE, N-COORD, N-PCSTATE apply to all SCCP subsystems/AEs via TC.

The TC primitives between the ASE and TC provide control of connectionless TCAP transactions. Service primitives for connection-oriented TC transactions are for further study.




| | |
|---|---|
| MTP-mgmt | MTP management primitives |
| MTP-trnfr | MTP primitives for message transfer |
| N-co | SCCP (network layer) connection oriented primitives |
| N-cl | SCCP (network layer) connectionless primitives |
| Functional interface | SCCP-ISUP interface for end to end signalling |
| TC-user | TC-user primitives for TCAP services |
| TC-mgmt | Management primitives for TC users |

*Note 1* – The handling of N-(management) primitives by TC is for further study.

*Note 2* – The handling of N-co primitives by TC is for further study.

FIGURE 8/Q.700

**Overview of the primitives used between the functional elements of CCITT No. 7**

## 5 Addressing

Addressing of CCITT S.S. No. 7 messages has to be considered on a number of levels. For example, the message transfer part uses the destination point code to route the message to the appropriate signalling point. The called party address field in TUP, or ISUP called party number field, in the Initial Address Message is used to route the call to the appropriate called destination. The capabilities of the various CCITT S.S. No. 7 addressing mechanisms are illustrated by the signalling message structure.

### 5.1 *Signalling message structure*

A signalling message is an assembly of information, defined at level 3 or 4, pertaining to a call, management transaction, etc., that is transferred as an entity by the message transfer function.

Each message contains service information including a service indicator identifying the source User Part and possibly additional information such as an indication whether the message relates to international or national application of the User Part.

The signalling information of the message includes the actual user information, such as one or more telephone or data call control signals, management and maintenance information, etc., and information identifying the type and format of the message. It also includes a label that provides information enabling the message to be:

- routed by the level 3 functions and thorugh a signalling network to its destination; and (This part of the label is known as the Routing label. This is shown in Figure 9/Q.700.)
- directed at the receiving User Part to the particular circuit, call, management or other transaction to which the message is related.

Further details are given in Q.700, § 5.2.

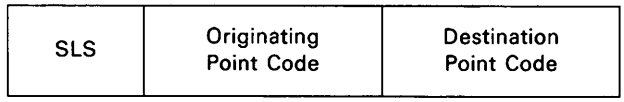



FIGURE 9/Q.700

**CCITT SS No. 7 Routing Label**

There are four types of label:

- type A for MTP management messages;
- type B for TUP;
- type C for ISDN-UP (circuit related) messages;
- type D for SCCP messages.

These are shown in Figure 10/Q.700.

The circuit identification code is used as a label for circuit related signalling messages, e.g., TUP or ISDN-UP. The least significant 4 bits of this field (in the TUP) is the Signalling Link Selection (SLS) field, which is used, where appropriate, to perform load sharing (see Q.704). In the ISDN-UP, the SLS is a separate field to the circuit identification code.

The CCITT No. 7 MTP signalling messages at level 2, which carry user information, are called Message Signal Units (MSUs). Figure 11/Q.700 shows the basic format of the MSU (refer also to Q.703) and the breakdown of the MSU. Signalling Information Field (SIF) when transporting circuit-related (ISDN-UP, TUP) messages and non-circuit-related messages (SCCP, TC based). Further details are given on message formats in Recommendations Q.704, Q.713, Q.723, Q.763, Q.773.

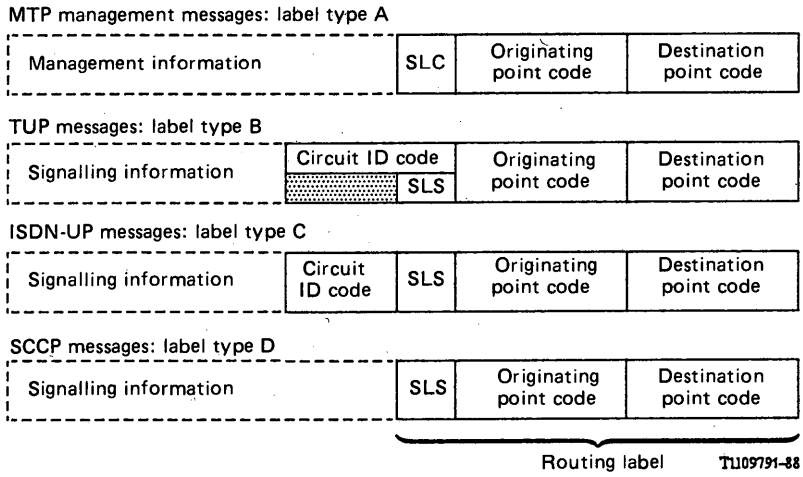



FIGURE 10/Q.700

**CCITT SS No. 7 message label types**

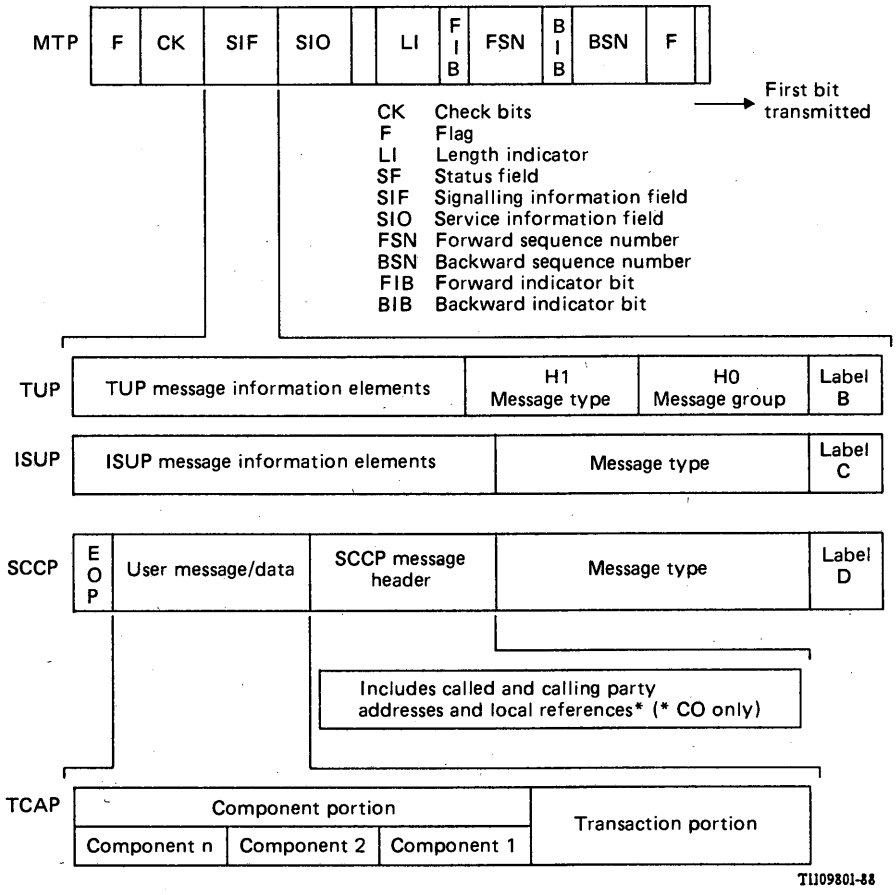



FIGURE 11/Q.700

**CCITT No. 7 signalling message structure**

## 5.2 *MTP addressing*

There is a two part addressing mechanism in the MTP, one part of the mechanism uses the point code which is incorporated in the routing label of every message signal unit, the other part of the mechanism makes use of the service indicator and network indicator within the service information octet. The point code is used for inter-node addressing and the SIO addresses signalling system users on an intra-node basis.

### 5.2.1 *Point codes*

Every signalling point (SP) and signalling transfer point (STP), when integrated in an SP, will be allocated its own unique point code. This is used by the MTP routing function to direct outgoing messages towards their destination in the network as indicated by the inclusion of the appropriate point code in the routing label. This point code is known as the destination point code (DPC). The routing label also contains the point code of the SP originating the message signal unit, therefore, the combination of this originating point code (OPC) and DPC will determine the signalling relation (i.e., the network points between which MTP "User" information is exchanged). The DPC is used by the receiving SP/STP discrimination function to determine whether the message is addressed to that SP or requires to be onward routed by means of the signal transfer capability of the STP.

The DPC will always be determined and inserted in the routing label by the level 4 MTP "User". This will also generally be the same for the OPC but it is possible that since the OPC might be constant it could be inserted by the MTP.

### 5.2.2 *Service indicator and network indicator*

The 4 bit service indicator (SI) and 2 bit network indicator (NI) are included in the service information octet (SIO) and are used within an SP's distribution function to determine the "User" the incoming message should be delivered to.

The SI will determine the "User", e.g., TUP, SCCP, ISUP and the NI will determine which network is concerned, e.g., international or national.

The NI will also in conjunction with the OPC/DPC determine whether a national or international signalling relation/routing is involved.

The NI, together with the standard 14 bit point code, allows for a max 16 384 point codes to be allocated in a signalling network.

## 5.3 *SCCP addressing*

Addressing within the SCCP of S.S. No. 7 makes use of three separate elements:

- DPC
- Global Title (GT)
- Sub-System Number (SSN)

One, two or all of the elements may be present in the Called and Calling Party Address, the main options are:

| | |
|---|---|
| GT<br>DPC + SSN | When transferring SCCP messages |
| SSN<br>GT<br>SSN + GT | When receiving messages from MTP |
| DPC<br>DPC + (SSN or GT or both)<br>GT<br>GT + SSn | When receiving messages from connectionless or connection-orientated control for SCCP Routing. |

The form of address used will depend on the service, application and underlying network.

5.3.1 *Global Title (GT)*

The Global Title (GT) may comprise of dialled digits or another form of address that will not be recognized in the S.S. No. 7 network, therefore, if the associated message requires to be routed over the S.S. No. 7 network, translation is required.

Translation of the GT will result in a DPC being produced and possibly also a new SSN and GT. A field is also included in the address indicator to identify the format of the global title.

5.3.2 *Destination Point Code (DPC)*

The DPC in an address requires no translation and will merely determine if the message is destined for that in SP (incoming message) or requires to be routed over the S.S. No. 7 signalling network via the MTP. For outgoing messages this DPC should be inserted in the MTP routing label. On an incoming message the DPC in the MTP routing label should correspond to the DPC in the called address.

5.3.3 *Subsystem Number (SSN)*

The SSN will identify a subsystem accessed via the SCCP within a node and may be a User Part, e.g., ISUP, SCCP management or an AE via TC. TC, however, will be invisible to the SCCP.

When examination of the DPC in an incoming message has determined that the message is for that SP, examination of the SSN will identify the concerned SCCP "User". The presence of an SSN without a DPC will also indicate a message which is addressed to that SP.

The SSN field has an initial capacity of 255 codes with an extension code for future requirements.

5.4 *User Part addressing*

5.4.1 *Telephone User Part addressing*

The Telephone User Part is capable of handling E.164 (incorporating E.163) addresses in the calling and called party address information elements.

5.4.2 *ISDN User Part addressing*

The ISDN User Part address structure is capable of handling E.164 addresses in the calling and called number, and re-directing address information elements.

5.4.3 *Signalling connection control part addresses*

The signalling connection control part is capable of handling E.164 (incorporating E.163), X.121, F.69, E.210, E.211, E.212, E.213, addresses, and the mobile hybrid E.214 address in the calling and called party address information elements.

The handling of OSI NSAP addresses in SCCP is for further study.

5.5 *Labelling*

A variety of methods to label signalling messages is used to allow the signalling system and users of the signalling system to relate a received message to a particular call or transaction.

For circuit-related messages, (e.g., on a simple telephone call), the TUP (and the ISUP) use the circuit identification code (CIC) to label the message.

For certain ISUP procedures, call reference are used to associate messages with calls.

SCCP also uses local references on connection oriented protocols.

Transaction capabilities use transaction and invoke identities to associate transaction messages and components respectively.

## 6 Operations administration and maintenance

### 6.1 *Management*

Management within S.S. No. 7 is partitioned into two main areas:

- Signalling network management;
- Signalling system management.

#### 6.1.1 *Signalling network management*

These are functions contained within the MTP and SCCP which, by means of automatic procedures, maintain the required signalling network performance (e.g., changeover of faulty links, forced re-routing, subsystem availability, etc.).

#### 6.1.2 *Signalling system management*

This may be considered as the actions taken by the operator (or by an external automatic mechanism) to maintain the signalling system performance when problems are identified.

#### 6.1.3 *Signalling System No. 7 and TMN*

The TMN concept identifies CCITT S.S. No. 7 as a candidate to act as a data communications network (DCN) for some TMN functions. The protocols that will be needed for this purpose are intended to be defined as ASEs, as part of OMAP. This topic is for further study.

#### 6.1.4 *Signalling System No. 7 and OSI management*

This subject is for further study.

### 6.2 *Maintenance and testing*

The maintenance administration and management functions of the signalling system themselves use the signalling system as a data carrying mechanism. When regarded in the data transport mode, however, any management or maintenance information is regarded as signalling traffic. Those functions having direct impact on S.S. No. 7 are included in OMAP Recommendation Q.795.

Testing within Signalling System No. 7 is:

- instigated automatically as a part of a signalling system management procedures (e.g., signalling route set test in MTP) or
- applied as a result of external activity, e.g., human-machine (MMI).

The first form is described in the appropriate Q.700 to Q.795 Recommendation dealing with MTP or SCCP, etc. The second form includes some MMI initiated procedures (initiation of MRVT (Q.795)), and also pre-in service testing using test cases specified in Recommendations for S.S. No. 7 tests (Q.780 to Q.783). A testing user part has been agreed to be necessary for pre-in service testing, this topic is for further study.

#### 6.2.1 *Operations Maintenance and Administration Part (OMAP)*

Recommendation Q.795 provides procedures and protocols related to operations and maintenance information. These procedures and protocols use TCAP and are invoked by the system management application process (SMAP). Recommendation Q.795 includes the following:

- MTP Routing Verification Test (MRVT)
- SCCP Routing Verification Test (SRVT) – for further study
- Circuit Validation Test

The protocol for the MRVT contained in Q.795 forms part of the OMAP AE which in turn uses the services provided by transaction capabilities.

ASEs needed to support the TMN functions are for further study.

6.2.2 *Testing*

Test specifications for Signalling System No. 7 are contained in Recommendations Q.780-783 and cover MTP level 2, level 3 and the TUP together with an overview of testing.

A Testing User Part is for further study.

6.3 *CCITT S.S. No. 7 measurements*

Recommendation Q.791 specifies the monitoring and measurements appropriate to the MTP and SCCP.

## 7 Signalling system performance

The performance requirements of Signalling System No. 7 must take account of the performance requirements of the services that are being supported. Each functional component of Signalling System No. 7 has its performance criteria specified in a self-contained Recommendation. An overall performance target is specified in the form of a Hypothetical Signalling Reference Connection (HSRC).

7.1 *Hypothetical Signalling Reference Connection (HSRC)*

The HSRC for Signalling System No. 7 (Recommendation Q.709), identifies components that are used in a signalling relation between signalling end points, signalling points, signalling transfer points, and signalling points with SCCP relay functions, and gives the values for the signalling delays and unavailability parameters. The values used are derived from the figures contained in the individual performance Recommendations for MTP, TUP, SCCP and ISUP.

7.2 *MTP*

The MTP signalling performance requirements are specified in Recommendation Q.706. This Recommendation includes:

- the parameters route-set unavailability, MTP malfunction (loss of messages and mis-sequencing), and message transfer times;
- factors affecting performance, for example signalling traffic characteristics (e.g., loading potential, security, etc.) and parameters related to transmission characteristics (e.g., bit rates of signalling data links);
- those parameters which have greatest influence on the signalling network queueing delays for example, error control, security arrangements, failures and priorities.

It should be noted that management functions affect MTP performance.

7.3 *SCCP*

The SCCP signalling performance requirements are contained in Recommendation Q.716. Parameters identified are signal connection delays (establishment, unsolicited reset, reset and release signalling connection, reset and release failure probability, data message transmit delay, data message delay failure and error probability and SCCP unavailability).

It should be noted that management functions affect SCCP performance.

7.4 *TUP*

The TUP signalling performance requirements are contained in Recommendation Q.725. Parameters contained in this Recommendation are cross office performance for TUP supported circuit connection control application under normal and abnormal traffic loads. Also specified is the probability of failure of calls due to signalling malfunction.

7.5 *ISDN-UP*

The ISDN-UP signalling performance requirements are contained in Recommendation Q.766. Parameters contained in this Recommendation are cross office performance for ISDN-UP supported circuit connection control under normal and abnormal traffic loads. Also specified is the probability of failure of an ISDN call due to signalling function.

## 8 Flow control

Signalling System No. 7 in common with other transport mechanisms, needs to limit the input of data when congestion onset is detected. Failure to do so can create overload situations. The nature of CCITT S.S. No. 7 will lead to SP/STP overload congestion being spread through the signalling network if no action is taken. This will result in impaired signalling performance. In addition to signalling network congestion within a node, congestion will also require action to prevent signalling performance from deteriorating. There is thus a need for flow control within the signalling system to maintain the required signalling performance.

### 8.1 *Signalling network flow control*

This is achieved by incorporating a flow control mechanism in the MTP. On detection of congestion, MTP "Users" are informed by the means of a special primitive; the "User" should then reduce signalling traffic towards the congested part of the network. If the User is at a remote SP, the information is carried across the network in an appropriate signalling network management message.

### 8.2 *Signalling node (congestion) flow control*

In addition to network congestion, nodal congestion also requires the remedial action of flow control to prevent the signalling performance from being impaired. Nodal congestion can occur both within the MTP and the MTP "User".

#### 8.2.1 *MTP nodal flow control*

A similar activity to that to combat signalling network congestion is required, i.e., on detection, the "User" is informed so that traffic can be reduced.

#### 8.2.2 *"User" flow control*

As well as taking action to reduce MTP congestion, mechanisms are also required within the User to detect the onset of congestion and to take appropriate action.

### 8.3 *Automatic congestion control*

The ISUP and TUP provide signalling procedures which aim to reduce the new calls offered to an exchange which is experiencing processor overload.

Automatic congestion control provides the means to inform adjacent exchanges of the current workload, and to request that only priority calls are offered to the exchange experiencing overload.

## 9 Compatibility mechanisms and rules in CCITT S.S. No. 7

### 9.1 *Modularity*

The wide scope of the signalling system requires that the total system include a large diversity of functions and that further functions can be added to cater for extended future applications. As a consequence only a subset of the total system may need to be used in an individual application.

A major characteristic of the signalling system is that it is specified with a functional structure to ensure flexibility and modularity for diverse applications within one system concept. This allows the system to be realized as a number of functional modules which could ease adaptation of the functional content of an operating Signalling System No. 7 to the requirements of its application.

The CCITT specifications of the signalling system specify functions and their use for international operation of the system. Many of those functions are also required in typical national applications. Furthermore, the system to some extent includes features that are particular to national applications. The CCITT specifications thus form an internationally standardized base for a wide range of national applications of common channel signalling.

CCITT S.S. No. 7 is one common channel signalling system. However, as a consequence of its modularity and its intended use as a standard base for national applications the system may be applied in many forms. In general, to define the use of the system in a given national application, a selection of the CCITT specified functions must be made and the necessary additional national functions must be specified depending on the nature of the application.

CCITT S.S. No. 7 is an evolutionary signalling system which has undergone a number of enhancements. To allow ease of evolution it has been necessary to incorporate a number of compatibility mechanisms in various functional elements of CCITT No. 7, and to apply a number of compatibility rules to protocol enhancement. Detailed specification of the compatibility mechanisms in each functional element of CCITT S.S. No. 7 are given in the appropriate Q.700 to Q.795 Recommendations. Hence an overview is given in this Recommendation.

Compatibility rules which apply to all functional elements of CCITT S.S. No. 7 are detailed in the following text.

### 9.2 *Evolutionary requirements*

In application protocols (e.g., ISDN-UP, ASEs), the main evolutionary requirement is the ability to add new subscriber services, new administration and network services to the protocol.

In the SCCP and MTP, the evolutionary requirements are different in that initial versions provide basic transport functions which are generally stable. The main enhancements have been in the management protocols.

Although the evolutionary requirements are different across the elements of CCITT S.S. No. 7, it is possible to incorporate certain common mechanisms in the various functional elements.

### 9.3 *Forward and backward compatibility*

Compatibility mechanisms can be considered as being either:

- Forward compatibility mechanisms
- Backward compatibility rules

Forward compatibility mechanisms are defined as a scheme to enable a version of a protocol to communicate effectively and interwork with future versions of the protocol.

Backward compatibility rules are defined as a scheme to ensure that future versions of the protocol will be able to send protocol messages to the previous version which will be understood and fully processed by the node supporting the previous version.

### 9.4 *Compatibility rules for CCITT S.S. No. 7*

The following compatibility rules are applied to each element of CCITT S.S. No. 7 (e.g., ISDN-UP) when protocols are enhanced.

#### 9.4.1 *Addition of a new value to an existing field (e.g., a cause value)*

New values to an existing field can be added. The processing of these new values at nodes supporting an earlier version of the protocol will be defined in their version specifications.

#### 9.4.2 *Addition of a new parameter to an existing message*

Any new parameters added to an existing message must not be added as mandatory parameters. If a new parameter, must be added, and it must be a mandatory parameter, then a new message type must be created.

#### 9.4.3 *Handling of unrecognized information*

When a new protocol, message or information element is created, a rule is required on a per message and information element basis, to define the action on receipt of unrecognized information. This rule needs to be applied to both unrecognized messages, unrecognized information elements within messages, and unrecognized values within recognized information elements.

The actions defined for receipt of an unrecognized message/information element could be:

- Discard message/information element.
- Discard/ignore information element within a recognized message.
- Default to a known general value (e.g., on receipt of an ISDN-UP IAM with an unrecognized calling party category could be defaulted to "Unknown").
- Send a "Confusion" message.
- Terminate the call/transaction.
- Information management.

### 9.4.4 *Increase in the length of optional parameters*

If a parameter is used as an optional parameter in all messages that it appears, the length of the parameter can be increased. The older version of the protocol would be able to function as it does today, assuming it ignores the extra bits or a suitable extension method has been defined. The newer version would have to check the length of the parameter to determine if the added information was present.

Protocols which use coding rules which are based on X.409 (e.g., TC) are not subject to this rule.

### 9.4.5 *Processing of messages with unrecognized SIO information*

To enable signalling points implemented to the Blue Book to interwork with signalling points implemented to earlier Recommendations when a message containing an unrecognized service information octet (see Q.704, § 14.2) is received, the message is discarded.

### 9.4.6 *Unacknowledged messages*

Where a function requires an acknowledgement to a message in order to continue, if no response is received the function sends the message for only a limited number of times. The sending signalling point should assume that the function is not available, and inform local management.

### 9.4.7 *Processing of spare fields*

For those CCITT S.S. No. 7 functions which define fields or sub-fields in signalling messages as spare or reserved, the following rules for processing of these fields apply.

At a node generating a signalling message, all spare and reserved fields are set to zero. At transit nodes, spare or reserved fields may be passed on transparently. At the destination node, the spare and reserved fields are not examined.

## 10 Glossary

A Glossary of terms in CCITT S.S. No. 7 is contained at the back of the Fascicles VI.7, VI.8 and VI.9.

SECTION 2

# MESSAGE TRANSFER PART (MTP)

**Recommendation Q.701**

## FUNCTIONAL DESCRIPTION OF THE MESSAGE TRANSFER PART (MTP) OF SIGNALLING SYSTEM No. 7

### 1 Introduction

#### 1.1 *General*

The Message Transfer Part (MTP) provides the functions that enable User Part significant information passed to the MTP to be transferred across the Signalling System No. 7 network to the required destination. In addition, functions are included in the MTP to enable network and system failures that would affect the transfer of signalling information to be overcome. This constitutes a sequenced connectionless service for the MTP user.

The Message Transfer Part together with one of its "users", the Signalling Connection Control Part (SCCP), described in Recommendations Q.711-716, forms the Network Service Part (NSP).

The Network Service Part meets the requirement for Layer 3 services as defined in the OSI – Reference Model CCITT Recommendation X.200. The relationship of the MTP with this model and to other parts of S.S. No. 7 is described in Recommendation Q.700.

#### 1.2 *Objectives*

The overall objectives of the Message Transfer Part are to provide the means for:

a) the reliable transport and delivery of "User Part" signalling information across the S.S. No. 7 network.

b) the ability to react to system and network failures that will affect a), and take the necessary action to ensure that a) is achieved.

The "Users" of MTP are the SCCP, Telephone User Part (TUP) [Recommendation Q.721-725 Data User Part (DUP) [Recommendation Q.741] and ISDN User Part (ISUP) [Recommendation Q.761-766]. The MTP Testing User Part is for further study.

#### 1.3 *General characteristics*

##### 1.3.1 *Method of description*

- functions provided by each level within the MTP
- services provided by the MTP
- interaction with the signalling network
- interaction with the MTP "User"
- the message transfer capability of the MTP

The functions of each level of the MTP are performed by means of the level protocol between two systems which provides a "level service" to the upper levels, (i.e., Level 1 Signalling Data Link, Level 2 Signalling Link and Level 3 Signalling network) as described in Recommendations Q.702, 703 and 704 respectively.

The service interface to the Level 4 "User" of MTP is described by means of primitives and parameters.

### 1.3.2 *Primitives*

Primitives consist of commands and their respective responses associated with the services requested of the SCCP and of the MTP, see Figure 1/Q.701. The general syntax of a primitive is shown below:

| X | Generic name | Specific name | Parameter |
|---|---|---|---|

- "X" designates the functional block providing the service ("MTP" for MTP).
- "Generic name" describes the action that should be performed by the addressed layer.
- "Specific name" indicates the direction of the primitive flow.
- "Parameters" are the elements of information which are to be transmitted between layers.

Four Specific Names exist in general:

- request
- indication
- response [1)]
- confirmation [1)]

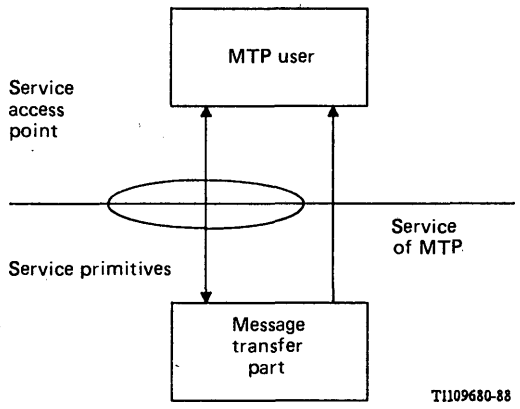



FIGURE 1/Q.701

**Service primitives**

[1)] Not all generic names contain all four specific names (Figure 2/Q.701).

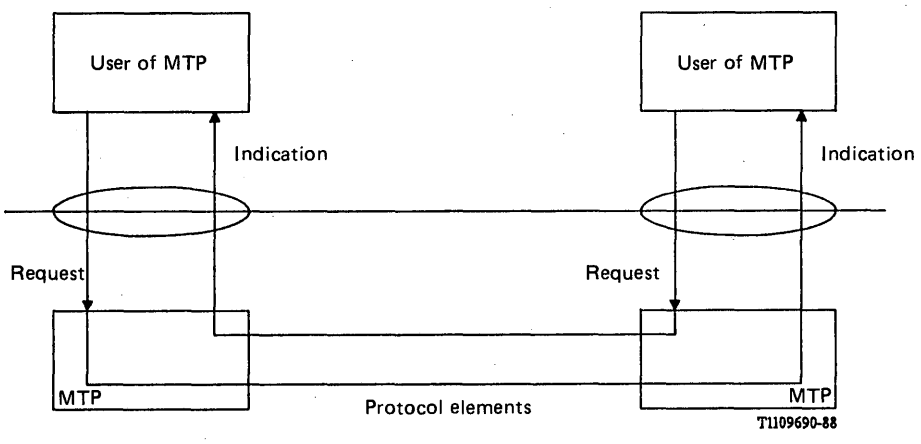



FIGURE 2/Q.701

**Specific name of primitives and peer to peer communication**

Primitives and parameters of the Messsage Transfer Part service are listed and described in Section 8 of this Recommendation.

1.3.3 *Peer-to-peer communication*

Exchange of information between two peers of the MTP is performed by means of a protocol. The protocol is a set of rules and formats by which the control information and MTP "User" data is exchanged between the two peers. The protocol caters for

- the transfer of "User" data in Message Signal Units (MSUs);
- level 2 control by use of Link Status Signal Units (LSSUs);
- testing and maintenance of signalling links by means of the signalling link test message carried in an MSU.

1.3.4 *Contents of Recommendations Q.701 to Q.707 Series relating to the MTP*

Recommendation Q.701 contains a functional description and overview of the Message Transfer Part of CCITT S.S. No. 7.

Recommendation Q.702 details the requirements of a signalling data link to support CCITT S.S. No. 7.

Recommendation Q.703 describes the signalling link functions.

Recommendation Q.704 describes signalling network functions and messages.

Recommendation Q.706 defines and specifies values for MTP performance parameters.

Recommendation Q.707 describes the testing and maintenance functions applicable to the MTP.

## 2 Signalling system structure

2.1 *Basic functional division*

The fundamental principle of the signalling system structure is the division of functions into a common Message Transfer Part (MTP) on one hand and separate User Parts for different users on the other. This is illustrated in Figure 3/Q.701.

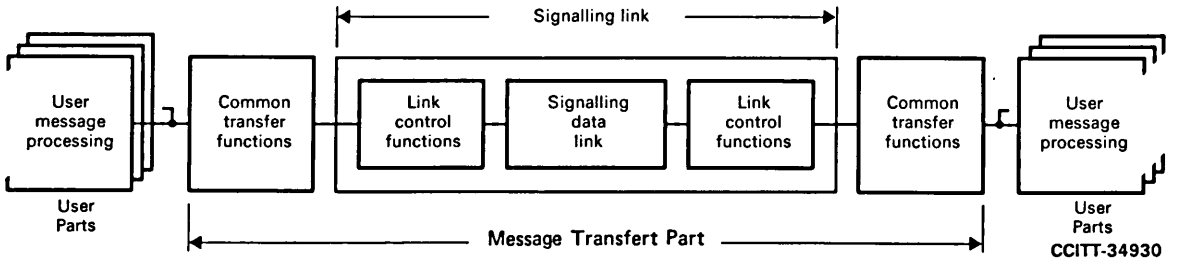



FIGURE 3/Q.701

**Functional diagram for the common channel signalling system**

The overall function of the Message Transfer Part is to serve as a transport system providing reliable transfer of signalling messages between the locations of communicating user functions.

The term *user* in this context refers to any functional entity that utilizes the transport capability provided by the Message Transfer Part. A User Part comprises those functions of, or related to, a particular type of user that are part of the common channel signalling system, typically because those functions need to be specified in a signalling context.

The basic commonality in signalling for different services resulting from this concept is the use of a common transport system, i.e., the Message Transfer Part. Also, a degree of commonality exists between certain User Parts, e.g., the Telephone User Part (TUP) and the Data User Part (DUP).

## 2.2 *Functional levels*

### 2.2.1 *General*

As a further separation, the necessary elements of the signalling system are specified in accordance with a level concept in which:

- the functions of the Message Transfer Part are separated into three functional levels, and
- the User Parts constitute parallel elements at the fourth functional level.

The level structure is illustrated in Figure 4/Q.701. The system structure shown in Figure 4/Q.701 is not a specification of an implementation of the system. The functional boundaries B, C and D may or may not exist as interfaces in an implementation. The interactions by means of controls and indications may be direct or via other functions. However, the structure shown in Figure 4/Q.701 may be regarded as a possible model of an implementation.

### 2.2.2 *Signalling data link functions (level 1)*

Level 1 defines the physical, electrical and functional characteristics of a signalling data link and the means to access it. The level 1 element provides a bearer for a signalling link.

In a digital environment, 64-kbit/s digital paths will normally be used for the signalling data link. The signalling data link may be accessed via a switching function, providing a potential for automatic reconfiguration of signalling links. Other types of data links, such as analogue links with modems, can also be used.

The detailed requirements for signalling data links are specified in Recommendation Q.702.

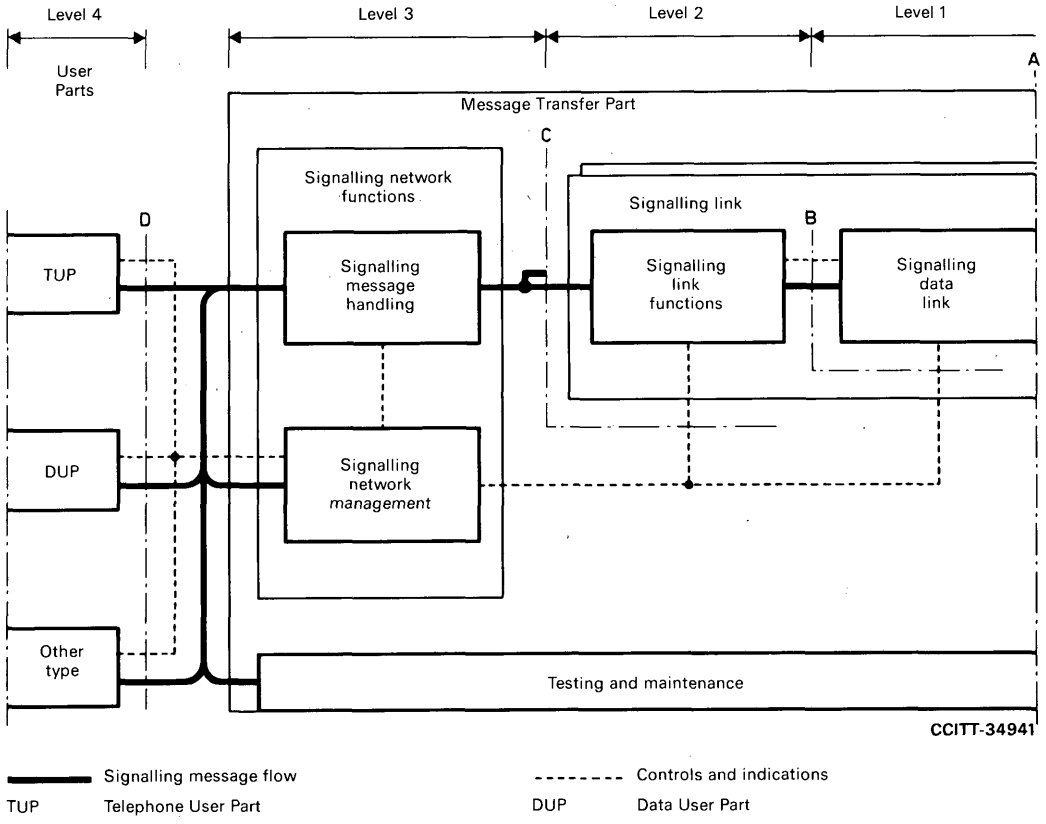



FIGURE 4/Q.701

**General structure of signalling system functions**

### 2.2.3 *Signalling link functions (level 2)*

Level 2 defines the functions and procedures for and relating to the transfer of signalling messages over one individual signalling data link. The level 2 functions together with a level 1 signalling data link as a bearer provides a signalling link for reliable transfer of signalling messages between two points.

A signalling message delivered by the higher levels is transferred over the signalling link in variable length *signal units*. For proper operation of the signalling link, the signal unit comprises transfer control information in addition to the information content of the signalling message.

The signalling link functions include:

- delimitation of signal unit by means of flags;
- flag imitation prevention by bit stuffing;
- error detection by means of check bits included in each signal unit;
- error correction by retransmission and signal unit sequence control by means of explicit sequence numbers in each signal unit and explicit continuous acknowledgements;
- signalling link failure detection by means of signal unit error rate monitoring and signalling link recovery by means of special procedures.

The detailed requirements for signalling link functions are given in Recommendation Q.703.

2.2.4 *Signalling network functions (level 3)*

Level 3 in principle defines those transport functions and procedures that are common to and independent of the operation of individual signalling links. As illustrated in Figure 4/Q.701 these functions fall into two major categories:

a) signalling message handling functions – these are functions that, at the actual transfer of a message, direct the message to the proper signalling link or User Part;

b) signalling network management functions – these are functions that, on the basis of predetermined data and information about the status of the signalling network, control the current message routing and configuration of signalling network facilities. In the event of changes in the status they also control reconfigurations and other actions to preserve or restore the normal message transfer capability.

The different level 3 functions interact with each other and with the functions of other levels by means of indications and controls as illustrated in Figure 4/Q.701. This figure also shows that the signalling network management as well as the testing and maintenance actions may include exchange of signalling messages with corresponding functions located at other signalling points. Although not User Parts these parts of level 3 can be seen as serving as "User Parts of the Message Transfer Part". As a convention in these specifications, for each description, general references to User Parts as sources or sinks of a signalling message implicitly include these parts of level 3 unless the opposite is evident from the context or explicitly stated.

A description of the level 3 functions in the context of a signalling network is given in § 3 below. The detailed requirements for signalling network functions are given in Recommendation Q.704. Some means for testing and maintenance of the signalling network are provided and the detailed requirements are given in Recommendation Q.707.

2.2.5 *User Part functions (level 4)*

Level 4 consists of the different User Parts. Each User Part defines the functions and procedures of the signalling system that are particular to a certain type of user of the system.

The extent of the User Part functions may differ significantly between different categories of users of the signalling system, such as:

– users for which most user communication functions are defined within the signalling system. Examples are telephone and data call control functions with their corresponding Telephone and Data User Parts;

– users for which most user communication functions are defined outside the signalling system. An example is the use of the signalling system for transfer of information for some management or maintenance purpose. For such an "external user" the User Part may be seen as a "mailbox" type of interface between the external user system and the message transfer function in which, for example, the user information transferred is assembled and disassembled to/from the applicable signalling message formats.

2.3 *Signalling message*

A signalling message is an assembly of information, defined at level 3 or 4, pertaining to a call, management transaction, etc., that is transferred as an entity by the message transfer function.

Each message contains *service information* including a *service indicator* identifying the source User Part and possibly additional information such as an indication whether the message relates to international or national application of the User Part.

The *signalling information* of the message includes the actual user information, such as one or more telephone or data call control signals, management and maintenance information, etc., and information identifying the type and format of the message. It also includes a *label* that provides information enabling the message:

– to be routed by the level 3 functions and through a signalling network to its destination; and

– to be directed at the receiving User Part to the particular circuit, call, management or other transaction to which the message is related.

On the signalling link, each signalling message is packed into Message Signal Units (MSUs) which also includes transfer control information related to the level 2 functions of the link.

2.4 *Functional interface*

The following functional interface between the Message Transfer Part and the User Parts can be seen as a model illustrating the division of functions between these parts. The interface (see Figure 5/Q.701) is purely functional and need not appear as such in an implementation of the system.

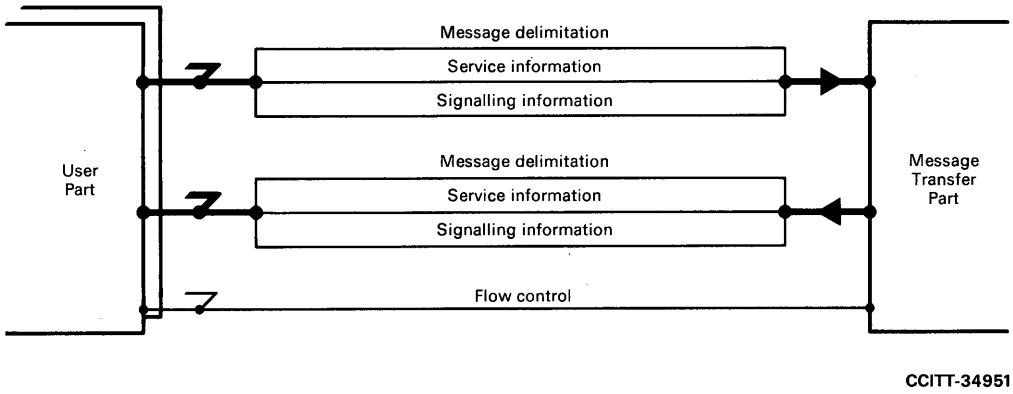



FIGURE 5/Q.701

**Functional interface between the message transfer part and the user parts**

The main interaction between the Message Transfer Part and the User Parts is the transfer of signalling messages across the interface, each message consisting of service information and signalling information as described above. Message delimitation information is also transferred across the interface with the message.

In addition to the transfer of messages and associated information, the interaction may also include flow control information, e.g., an indication from the Message Transfer Part that it is unable to serve a particular destination.

A description of the characteristics of the Message Transfer Part as seen from the functional interface and the requirements to be met by potential users of the message transfer function is given in § 4.

## 3 Message transfer part and the signalling network

### 3.1 *General*

Since the Message Transfer Part forms the interface at a node with the rest of the signalling network, the signalling network will have significant impact on the MTB. The MTP must however be independent of the signalling network in that it has to be capable of performing its set functions and attaining its objectives no matter what network structure or status prevails.

The MTP has therefore to contain the necessary functions to ensure any impact that the network has does not impair MTP performance.

#### 3.1.1 *Signalling network components*

A full description of signalling network components is contained in Recommendation Q.700, the components that must be considered by the MTP are:

- signalling points (including signalling transfer points);
- signalling relations between two signalling points;
- signalling links;
- signalling link sets (including link groups);
- signalling routes;
- signalling route-sets.

#### 3.1.2 *Signalling modes*

Signalling modes are described in Recommendations Q.700 and Q.705 (signalling network structures). The modes applicable to CCITT S.S. No. 7 MTP are:

- associated mode;
- quasi-associated mode.

### 3.1.3 *Signalling point modes*

A signalling point can be an originating point, a destination point or a signalling transfer point in a signalling relation. All three modes must be considered in the MTP.

### 3.1.4 *Message labelling*

Each message contains a label. In the standard label the portion that is used for routing is called the *routing label.* This routing label includes:

a) explicit indications of destination and originating points of the message, i.e., identification of the signalling relation concerned;

b) a code used for load sharing which may be the least significant part of a label component that identifies a user transaction at level 4.

The standard routing label assumes that each signalling point in a signalling network is allocated a code according to a code plan, established for the purpose of labelling, that is unambiguous within its domain. Messages labelled according to international and national code plans are discriminated by means of an indication in the service information octet included in each message.

The standard routing label is suitable for national applications also. However, the signalling system includes the possibility for using different routing labels nationally.

## 3.2 *Signalling message handling functions*

Figure 6/Q.701 illustrates the signalling message handling functions.

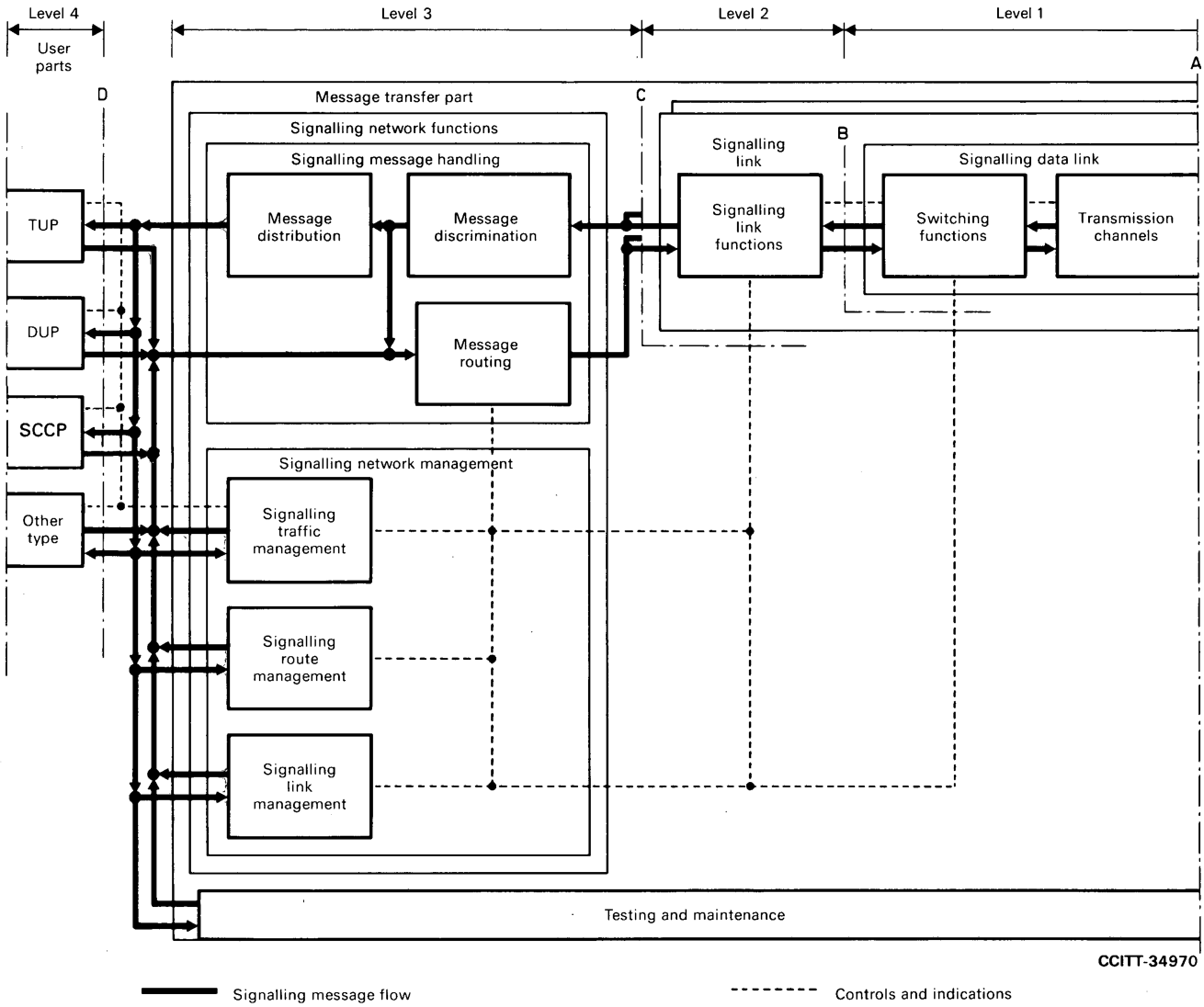



FIGURE 6/Q.701

**Detailed structure of signalling system functions**

3.2.1 *Message routing*

*Message routing* is the process of selecting, for each signalling message to be sent, the signalling link to be used. In general, message routing is based on analysis of the routing label of the message in combination with predetermined routing data at the signalling point concerned.

Message routing is destination-code dependent with typically an additional load-sharing element allowing different portions of the signalling traffic to a particular destination to be distributed over two or more signalling links. This traffic distribution may be limited to different links within a link set or applied to links in different link sets.

Each succession of signalling links that may be used to convey a message from the originating point to the destination point constitutes a *message route.* A signalling route is the corresponding concept for a possible path referring to a succession of link sets and signalling transfer points, between a given signalling point and the destination point.

In Signalling System No. 7, message routing is made in a manner by which the message route taken by a message with a particular routing label is predetermined and, at a given point in time, fixed. Typically, however, in the event of failures in the signalling network, the routing of messages, previously using the failed message route, is modified in a predetermined manner under control of the signalling traffic management function at level 3.

Although there are in general advantages in using a uniform routing of messages belonging to different User Parts, the service indicator included in each message provides the potential for using different routing plans for different User Parts.

3.2.2 *Message distribution*

*Message distribution* is the process which, upon receipt of a message at its destination point, determines to which User Part or level 3 function the message is to be delivered. This choice is made on analysis of the service indicator.

3.2.3 *Message discrimination*

*Message discrimination* is the process which, upon receipt of a message at a signalling point, determines whether or not the point is the destination point of that message. This decision is based on analysis of the destination code in the routing label in the message. If the signalling point is the destination point the message is delivered to the message distribution function. If it is not the destination point, and the signalling point has the transfer capability, the message is delivered to the routing function for further transfer on a signalling link.

3.3 *Signalling network management functions*

Figure 6/Q.701 illustrates the signalling network management functions.

3.3.1 *Signalling traffic management*

The tasks of the *signalling traffic management* function are:

a) to control message routing; this includes modification of message routing to preserve, when required, accessibility of all destination points concerned or to restore normal routing;

b) in conjunction with modifications of message routing, to control the resulting transfer of signalling traffic in a manner that avoids irregularities in message flow;

c) flow control.

Control of message routing is based on analysis of predetermined information about all allowed potential routing possibilities in combination with information, supplied by the *signalling link management* and *signalling route management* functions, about the status of the signalling network (i.e., current availability of signalling links and routes).

Changes in the status of the signalling network typically result in modification of current message routing and thus in transfer of certain portions of the signalling traffic from one signalling link to another. The transfer of signalling traffic is performed in accordance with specific procedures. These procedures – *changeover, changeback, forced rerouting and controlled rerouting* – are designed to avoid, as far as the circumstances permit, such irregularities in message transfer as loss, mis-sequencing or multiple delivery of messages.

The changeover and changeback procedures involve communication with other signalling point(s). For example, in the case of changeover from a failing signalling link, the two ends of the failing link exchange information (via an alternative path) that normally enables retrieval of messages that otherwise would have been lost on the failing link. However, as further explained later, these procedures cannot guarantee regular message transfer in all circumstances.

A signalling network has to have a signalling traffic capacity that is higher than the normal traffic offered. However, in overload conditions (e.g., due to network failures or extremely high traffic peaks) the signalling traffic management function takes flow control actions to minimize the problem. An example is the provision of an indication to the local user functions concerned that the Message Transfer Part is unable to transport messages to a particular destination in the case of total breakdown of all signalling routes to that destination point. If such a situation occurs at a signalling transfer point, a corresponding indication is given to the signalling route management function for further dissemination to other signalling points in the signalling network.

### 3.3.2 *Signalling link management*

The task of the signalling link management function is to control the locally connected link sets. In the event of changes in the availability of a local link set it initiates and controls actions aimed at restoring the normal availability of that link set.

The signalling link management function also supplies information about the availability of local links and link sets to the signalling traffic management function.

The signalling link management function interacts with the signalling link function at level 2 by receipt of indications of the status of signalling links. It also initiates actions at level 2 such as, for example, initial alignment of an out-of-service link.

The signalling system can be applied with different degrees of flexibility in the method of provision of signalling links. A signalling link may for example consist of a permanent combination of a signalling terminal device and a signalling data link. It is also possible to employ an arrangement in which any switched connection to the remote end may be used in combination with any local signalling terminal device. It is the task of the signalling link management function in such arrangements to initiate and control reconfigurations of terminal devices and signalling data links to the extent such reconfigurations are automatic. In particular, this involves interaction, not necessarily direct, with a switching function at level 1.

### 3.3.3 *Signalling route management*

Signalling route management is a function that relates to the quasi-associated mode of signalling only. Its task is to transfer information about changes in the availability of signalling routes in the signalling network to enable remote signalling points to take appropriate signalling traffic management actions. Thus a signalling transfer point may, for example, send messages indicating inaccessibility of a particular signalling point via that signalling transfer point, thus enabling other signalling points to stop routing messages to an incomplete route.

## 3.4 *Testing and maintenance functions*

Figure 6/Q.701 illustrates that the signalling system includes some standard testing and maintenance functions that use level 3 messages. Furthermore, any implementation of the system typically includes various implementation-dependent means for testing and maintenance of equipment concerned with the other levels.

## 3.5 *Use of the signalling network*

### 3.5.1 *Signalling network structure*

The signalling system may be used with different types of signalling network structures. The choice between different types of signalling network structures may be influenced by factors such as the structure of the telecommunication network to be served by the signalling system and administrative aspects.

In the case when the provision of the signalling system is planned purely on a per-signalling relation basis, the likely result is a signalling network largely based on associated signalling, typically supplemented by a limited degree of quasi-associated signalling for low volume signalling relations. The structure of such a signalling network is mainly determined by the patterns of the signalling relations. International signalling is an example of an application for which this approach is suitable.

Another approach is to consider the signalling network as a common resource that should be planned according to the total needs for common channel signalling. The high capacity of digital signalling links in combination with the need for redundancy for reliability, typically leads to a signalling network based on a high degree of quasi-associated signalling with some provision for associated signalling for high-volume signalling relations. The latter approach to signalling network planning is more likely to allow exploitation of the potential of common channel signalling to support network features that require communication for purposes other than the switching of connections.

Further considerations about the use of a signalling network are given in Recommendation Q.705.

### 3.5.2 *Provision of signalling facilities*

In general, the most important factor in the dimensioning of the signalling network is the need for reliability by means of redundancy. Depending on the signalling network structure and the potential for reconfiguration of signalling equipment, the required redundancy may be provided by different combinations of:

- redundancy in signalling data links (e.g., nominated reserves or switched connections);
- redundancy in signalling terminal devices (e.g., a common pool of terminals for the whole signalling point);
- redundancy of signalling links within a link set (typically operating with load sharing);
- redundancy in signalling routes for each destination (possibly operating with load sharing).

The loading capacity of a digital signalling link is high in relation to the signalling traffic generated for call control signalling. Therefore, in many typical applications the links will be lightly loaded and signalling traffic volume will be a secondary factor in the dimensioning of the signalling network. However, in high signalling traffic applications or when analogue links with lower speeds are used, it may be necessary to dimension the traffic capacity by provision of additional signalling links. The message routing principles adopted for the signalling system allow partitioning of the total signalling traffic into different portions based on load sharing, destination point code and service information. Such partitioning provides a useful means of controlling the load and dimensioning of the capacity of different sections of a signalling network as it allows distribution of different portions of the signalling traffic. It can also be used to dedicate certain parts of a signalling network to signalling traffic related to a particular user.

### 3.5.3 *Application of signalling network functions*

The signalling network functions provided by the signalling system are designed to cater for a range of signalling network configurations. It is not necessary that all of those functions be present at all signalling points. The necessary functional content at level 3 at a particular signalling point depends for example on what signalling mode(s) are used, whether or not it is a signalling transfer point, what type of signalling equipment redundancy is employed, etc. It is thus feasible to implement level 3 functions with modularity for different capabilities corresponding to different signalling network configurations. As a special case, it is even possible to apply the signalling system without using the level 3 element at all, e.g., in a small exchange or private automatic branch exchange which can only be reached via one primary pulse code modulation system.

## 4 Message transfer capability

### 4.1 *General*

The Message Transfer Part recommendations specify methods by which different forms of signalling networks can be established. The requirements for the Message Transfer Part have been determined primarily by the requirements of call control signalling for the telephone and circuit switched data transmission services. However, the Message Transfer Part is also intended to have the ability to serve as a transport system for other types of information transfer. The following summarises the typical characteristics of the transport service that may be offered by the Message Transfer Part to a potential user of this ability.

All information to be transferred by the Message Transfer Part must be assembled into messages. The linking of the source and sink of a message is inherent in the label in combination with the signalling routes existing between the two locations. From a transportation point of view each message is self-contained and handled individually. The nature of the transport service offered by the Message Transfer Part is therefore similar to that offered by a packet switched network. In addition, all messages containing the same label constitute a set of messages that is handled in a uniform manner by the Message Transfer Part, thus ensuring, in normal circumstances, regular delivery in the correct sequence.

### 4.2 *User location in system structure*

A potential user of the transport service is typically included in the system structure by provision of a separate User Part. This requires allocation of a service indicator code, the specification of which is part of both the Message Transport Part and User Part concerned.

As an alternative, a potential user may be catered for, together with other similar users, by an already existing or new User Part. In such a case the discrimination between messages belonging to this potential user and the other similar users is an internal matter within the User Part concerned. It then follows that all messages belonging to such a User Part are necessarily handled, e.g., as regards routing, in a uniform manner by the Message Transfer Part.

### 4.3 *Message content*

#### 4.3.1 *Code transparency*

Information with any code combination generated by a user can be transferred by the Message Transfer Part provided that the message respects the requirements described below.

#### 4.3.2 *Service information*

Each message must contain service information coded in accordance with the rules specified in Recommendation Q.704, § 14.

#### 4.3.3 *Message label*

Each message must contain a label consistent with the routing label of the signalling network concerned. See also Recommendation Q.704, § 2.

#### 4.3.4 *Message length*

The information content of a message should be an integral number of octets.

The total amount of signalling information transferable in one message is limited by some parameters of the signalling system; the signalling system can accept transfer of user information blocks in the order of 256 octets in single messages.

Depending on the signalling traffic characteristics of a user and of other users sharing the same signalling facilities, there may be a need to limit message lengths below the system limit based on queueing delay considerations.

In the case when information blocks generated by a user function exceed the allowed message length, it is necessary to implement means for segmentation and blocking of such information blocks within the User Part concerned.

### 4.4 *User accessibility*

The accessibility of user functions through a signalling network depends on the signalling modes and routing plan employed in that network.

In the case when only the associated mode of signalling is employed, only user functions located at adjacent signalling points may be accessed.

In the case when quasi-associated signalling is employed, user functions located at any signalling point may be accessed provided that the corresponding message routing data is present.

### 4.5 *Transport service performance*

Further detailed information is provided in Recommendation Q.706.

#### 4.5.1 *Message transfer delay*

The normal delay for transfer of messages between user locations depends on factors such as distance, signalling network structure, signalling data link type and bit rate and processing delays.

A small proportion of messages will be subject to additional delay because of transmission disturbances, network failures, etc.

#### 4.5.2 *Message transfer failures*

The Message Transfer Part has been designed to enable it to transfer messages in a reliable and regular manner even in the presence of network failures. However, inevitably some failures will occur the consequences of which cannot be avoided with economic measures. The types of failures that may occur and some typical probabilities of their occurrence are described below. Recommendation Q.706 provides further detailed information that can be used to estimate failure rates for particular cases.

In the case when a potential user function requires a reliability of the transport service that cannot be guaranteed by the Message Transfer Part, the reliability of that user may be enhanced by adoption of appropriate level 4 procedures, possibly including some means of supplementary end-to-end error control.

The following types of message transfer failures are possible, and the expected probabilities for such failures in typical applications are indicated (see also Recommendation Q.706).

a) Unavailability of the transport service to one or more locations – the availability of the message transfer capability depends on the redundancy provided in the signalling network; the availability can therefore be dimensioned.

b) Loss of messages – the probability of loss of messages mainly depends on the reliability of signalling equipment; typically it is expected to be lower than $10^{-7}$.

c) Mis-sequencing of messages – may in certain configurations of quasi-associated signalling occur with rare combinations of independent failures and disturbances. The probability, in such configurations, of a message being delivered out-of-sequence depends on many factors but is expected to be lower than $10^{-10}$.

d) Delivery of false information – undetected errors may lead to the delivery of false information; the possibility of an error in a message delivered is expected to be lower than $10^{-10}$.

## 5 Differences from the Red Book

The ongoing development of the MTP during this study period has resulted in a number of differences occurring between the Recommendations as documented in the Red Book and these current Recommendations (Blue Book). In order to limit interworking problems, a backwards compatibility mechanism is required (see § 6). As an initial step towards producing such a mechanism, this section identifies the new items and items changed because of operational considerations, that have been included in the Blue Book. This section does not consider editorial or technical corrections.

### 5.1 *Signalling Information Field length*

The maximun length of the Signalling Information Field has been increased to 272 octets. This was previously a National only option. Networks using both signalling terminals with 62 octet maximum SIF length handling capability and signalling terminals with 272 octet maximum SIF length handling capability must ensure that messages with SIFs longer than 62 octets cannot be routed to signalling links that are unable to handle them (see § 7).

### 5.2 *Signalling Point Restart*

The Signalling Point Restart procedure (see Q.704 § 9) has been included together with a definition of Signalling Point availability. This procedure allows a graceful increase in message traffic at a restarting Signalling Point.

5.3 *Management Blocking*

The Management Blocking procedure for Signalling links has been deleted. No interworking problems are foreseen in networks where some Signalling Points still incorporate this procedure and others are implemented in accordance with the Blue Book.

5.4 *Signalling Link Test*

The Signalling Link Test has been enhanced to check that both ends of the link agree as to which signalling link is being tested. No interworking problems are foreseen (see Q.707 § 2.2).

5.5 *Compatibility mechanism*

General principles have been incorporated in the Message Transfer Part that will allow implementations to the Blue Book to be compatible with implementations to Red/Yellow Books and future issues of the Recommendations (see § 6).

5.6 *Timer values*

The values of existing Q.703 and Q.704 Timers have been finalized (see § 7).

5.7 *Processor Outage*

The actions related to Processor Outage have been clarified (see Q.703 § 8 and Q.704 § 4, 5 and 6). No interworking problems are foreseen.

5.8 *User flow control*

Procedures for Message Transfer Part User Flow Control have been adopted for use at a Signalling Point when an MTP user has become unavailable (see Q.704 § 11 and Q.701 § 7).

5.9 *Management Inhibiting and Management Inhibiting test procedure*

The time-controlled changeover procedure is now used to divert traffic from a management inhibited link.

To verify the inhibited status of a link, test procedures have been introduced into management inhibiting (see Q.704 § 10 and Q.701 § 7).

5.10 *Signalling point/signalling transfer point congestion*

Procedures to detect and handle signalling point/signalling transfer point congestion have now been identified (see Q.704 § 11.2.6). No interworking problems are foreseen.

## 6 Compatibility in the message transfer part

To enable implementations of Signalling System No. 7 to this issue (Blue Book) of the Recommendations to achieve compatibility with implementations to other issues, e.g., Yellow, Red and 1992 Books, a set of appropriate procedures and guidelines has been concluded in Recommendation Q.700. This section identifies the action that is required within the Message Transfer Part to ensure both forward and backwards compatibility. The areas considered are the treatment of spare fields, spare values, lack of acknowledgements and unreasonable information.

6.1 *Unreasonable Information*

The following actions occur in the MTP when messages are received containing unreasonable information.

6.1.1 *Messages containing an unallocated SIO value*

When messages containing an unallocated SIO value are received at either a terminating Signalling Point or an STP that employs message routing based on both DPC and SIO, they should be discarded. If required, a report should be made to management.

6.1.2 *Messages containing an unallocated H0/H1 code*

When messages containing an unallocated H0/H1 code are received at the appropriate functional block within the MTP, they are discarded. There should be no impact on any protocol and, if required, a report should be made to management.

6.1.3 *Messages containing an unallocated value in a recognized field*

When massages are received at an owning function within the MTP containing a field with an unallocated value they are discarded and, if required, a report made to management. There should be no impact on any current protocol.

(An owning function is a function to which a received message pertains.)

6.2 *Treatment of spare fields*

The MTP will handle spare fields in MTP messages in the following manner:

i) Spare fields are set to zero on message creation, and are not examined on reception at the destination owning function.

ii) Spare subfields are set to zero on message creation, and are not examined on reception at the destination owning function.

iii) Implementations of the STP function should transit all messages unchanged, including spare fields and spare subfields.

6.3 *Lack of acknowledgement*

Should a message that requires an acknowledgement not receive one within a specified time, the message will be repeated, unless the protocol specifies otherwise. However, subsequent failures to receive the acknowledgement should not cause indefinite repeat attempts.

## 7 Interworking of Yellow, Red and Blue MTP implementations

There have been a number of changes introduced into this issue (Blue Book) of Recommendations Q.701-707 from the previous issue (Red Book). The changes have been identified in § 5 and although in the majority of cases there will be no interworking problems between a Signalling Point/STP implemented to the Red Book and one implemented to a Blue Book, there are some instances where problems will arise. This section gives guidance on the appropriate action that can be taken in the MTP to overcome interworking problems and also considers Yellow to Red Book and Yellow to Blue Book interworking.

7.1 *Yellow Book to Red Book interworking*

There were four areas where changes from the Yellow Book to the Red Book introduced interworking problems:

i) Level 2 flow control, LSSU SIB introduced.

ii) Transfer Restricted (TRF) and Transfer Controlled (TFC) messages and procedures were introduced into the Red Book.

iii) Transfer Allowed (TAA) and Transfer Prohibited (TPA) acknowledgements were deleted from the Red Book.

iv) Management inhibiting procedures were introduced into the Red Book.

The suggested action required at the Yellow and/or Red Book SP/STP to enable interworking is contained in the following point items.

7.1.1 *Level 2 Flow control*

The Red Book SP/STP should apply normal level 2 flow control action (i.e., acknowledgements are withheld and SIBs sent). The Yellow Book SP/STP should ignore the LSSU SIB when received. It is recognized that although flow control is not performed in this case, interworking is possible. However, a possible option would be to set the congestion threshold at the Red Book SP/STP, such that flow control is not triggered on that signalling relation.

7.1.2 *Transfer restricted and Transfer controlled procedures*

The Yellow Book SP/STP should ignore TFR and TFC messages when received.

7.1.3 *Transfer allowed/Transfer prohibited acknowledgements*

The Yellow Book SP/STP should limit the repetition of the TFA/TFP message to once only. The Red Book SP/STP should ignore the acknowledgement messages when they are received.

7.1.4 *Management inhibiting procedure*

The Yellow Book SP/STP should ignore the Link Inhibit (LIN) and Link Uninhibit (LUN) messages when received. The Red Book SP/STP should limit the repetition of the LIN/LUN message.

7.2 *Red Book to Blue Book interworking*

The changes in this issue (Blue Book) from the Red Book Q.701-707 Recommendations are identified in § 5. There are five areas where changes have resulted in interworking problems:

i) Signalling Point Restart procedure has introduced the Traffic Restart Allowed (TRA) message.

ii) Timer values have been confirmed in this issue, previous values were provisional.

iii) User Flow Control procedure has introduced the User Part Unavailable (UPU) message.

iv) Signalling Information Field length increase will require action to prevent overlength messages being sent on a link that is not capable of handling them.

v) Management-inhibiting test procedure has introduced Link Local inhibit test message (LLT) and Link Remote inhibit test message (LRT).

The suggested actions required at the Red and/or Blue Book SP/STP to enable interworking are contained in the following point items.

7.2.1 *Signalling Point Restart*

The Red Book SP/STP should ignore the Traffic Restart Allowed messages when received.

7.2.2 *Q.703 and Q.704 timer values*

Where possible, an SP/STP implemented to the Red Book should adopt the timer values specified in the Blue Book when interworking with a Blue Book SP/STP. For timer values (see Q.703 § 12 and Q.704 § 16).

7.2.3 *User flow control*

The Red Book SP/STP should ignore the User Part Unavailable (UPU) message if received.

7.2.4 *Management inhibit test procedure*

The Red Book SP/STP should ignore the Link Local inhibit test (LLT) and Link Remote inhibit test (LRT) messages. A report to local management should also be made.

7.2.5 *SIF length increase*

The SP/STP with 272 octet SIF length handling capability should prevent overlength messages from being routed over signalling links that only have a 62 octet SIF handling capability.

7.2.6 *SIF length increase (National networks option)*

In the international Signalling System No. 7 network, it should be possible to identify signalling links/routes with a limited SIF length handling capability and prevent overlength messages being transmitted over them by administrative action based on the exchange of operational data. However, with some national networks due to the rapid change in status of SP/STP implementation level (e.g., 62 to 272 SIF capability) and the number of SP/STPs in the network, this administrative action and data exchange may not be adequate. In this situation, a mechanism based on the following MTP activities may be more appropriate.

i) Detection of a link with 272 SIF capability may be achieved by coding the "D" bit of LSSUs sent during alignment as 1 (with 62 octet SIF links it would be 0). On receipt of this LSSU, a Blue Book SP/STP would mark the link/route as having 272 SIF capability. A Red Book SP/STP would ignore the coding of the "D" bit and treat the LSSU in the normal manner.

ii) When a Blue Book SP/STP receives a message for onward routing, it will check if the message (SIF) is greater than 62 octets. If the SIF is greater than 62 octets, it will verify that the link/route can handle a message of this length. Should the link/route not have the SIF length capability, the message will be discarded and an indication sent to the message origin. A Red Book SP/STP should not receive a message with an SIF $>$ 62 octets.

iii) If the message originator is a local MTP User, an MTP PAUSE primitive will be returned by the MTP in response to an overlength message (see § 8). Should the originator be at a remote SP, a TFA coded to indicate that only 62 octet SIF messages can be transferred will be returned by the MTP in response to an overlength message (see Q.704 § 15).

In national networks using an SIF compatibility mechanism, the two spare bits in the TFA (see Q.704 § 15.8.2) may be coded as an SIF compatibility indicator as follows:

bit B A

0 0 Allow 62 octet SIFs/Prohibit 272, X and Y octet SIFs

0 1 Allow 62 and 272 octet SIFs/Prohibit X and Y octet SIFs

1 0 Allow 62, 272 and X octet SIFs Prohibit Y octet SIFs.

1 1 Allow 62, 272, X and Y octet SIFs.

*Note* – 272 $<$ X $<$ Y octets, the values of X and Y are for further study.

7.3 *Yellow Book to Blue Book Interworking*

The changes between Yellow and Blue Books have taken place in two stages: Yellow to Red and Red to Blue. Therefore, to achieve interworking between Yellow and Blue Book implementations, the actions specified in §§ 7.1 and 7.2 should be applied. In § 7.1 Red Book SP/STP should be read as Blue Book SP/STP and in § 7.2 Red Book SP/STP should be read as Yellow Book SP/STP.

There is one change from the Red Book in the Blue Book that will have an additional impact on interworking with the Yellow Book, and that is the deletion of the blocking procedure. This means that while a Yellow Book implementation can block a signalling link, a Blue Book node can neither inhibit nor block the link in the opposite direction.

## 8 Primitives and Parameters of the Message Transfer Part

The primitives and parameters are shown in Table 1/Q.701.

TABLE 1/Q.701

**Message transfer part service primitives**

| Primitives | | Parameters |
|---|---|---|
| Generic Name | Specific Name | |
| MTP-TRANSFER | Request Indication | OPC (see Q.704 § 2.2)<br>DPC (see Q.704 § 2.2)<br>SLS (see Q.704 § 2.2) (Note 1)<br>SIO (see Q.704 § 14.2)<br>User data (see Q.703 § 2.3.8) |
| MTP-PAUSE<br>(Stop) | Indication | Affected DPC |
| MTP-RESUME<br>(Start) | Indication | Affected DPC |
| MTP-STATUS | Indication | Affected DPC Cause (Note 2) |

*Note 1* – The MTP users should take into account that this parameter is used for load sharing by the MTP, therefore, the SLS values should be distributed as equally as possible. The MTP guarantees (to a high degree of probability) an in-sequence delivery of messages which contain the same SLS code.

*Note 2* – The Cause parameter has, at present, two values:

i) *Signalling network congested (level)*

This parameter value is included if national options with congestion priorities and multiple signalling link states without congestion priorities as in Recommendation Q.704 are implemented.

ii) *Remote User unavailable.*

### 8.1 *Transfer*

The primitive "MTP-TRANSFER" is used between level 4 and level 3 (SMH) to provide the MTP message transfer service.

### 8.2 *Pause*

The primitive "MTP-PAUSE" indicates to the "Users" the total inability of providing the MTP service to the specified destination.

### 8.3 *Resume*

The primitive "MTP-RESUME" indicates to the "User" the total ability of providing the MTP service to the specified destination.

This primitive corresponds to the destination accessible state as defined in Recommendations Q.704.

8.4 *Status*

The primitive "MTP-STATUS" indicates to the "Users" the partial inability of providing the MTP service specified destination. The primitive is also used to indicate to a User that a remote corresponding User is unavailable (see Q.704 § 11.2.7).

In the case of national option with congestion priorities or multiple signalling link congestion states without priorities as in Recommendation Q.704 are implemented, this "MTP-STATUS" primitive is also used to indicate a change of congestion level.

This primitive corresponds to the destination congested/User Part unavailable state as defined in Recommendation Q.704.

8.5 *Restart*

The MTP indicates to the "Users" at the restarting SP that the MTP is commencing or ending the signalling point restart procedure (see Recommendation Q.704, § 9).

The indication may have the following qualifiers:

i) Begin

ii) End

The qualifier "Begin" indicates to the "Users" that all destinations should be marked as accessible (but that the resumption of signalling traffic must await the reception of MTP-RESUME primitive or MTP restart indication "End").

The qualifier "End" indicates to the "Users" that signalling traffic may be restarted, taking into account any MTP-PAUSE primitives previously received.

The means of conveying the MTP restart indication to the MTP "Users", is for further study.

**Recommendation Q.702**

## SIGNALLING DATA LINK

### 1 General

1.1 A *signalling data link* is a bidirectional transmission path for signalling, comprising two *data channels* operating together in opposite directions at the same data rate. It constitutes the lowest functional level (level 1) in the Signalling System No. 7 functional hierarchy.

1.2 Functional configuration of a signalling data link is shown in Figure 1/Q.702.

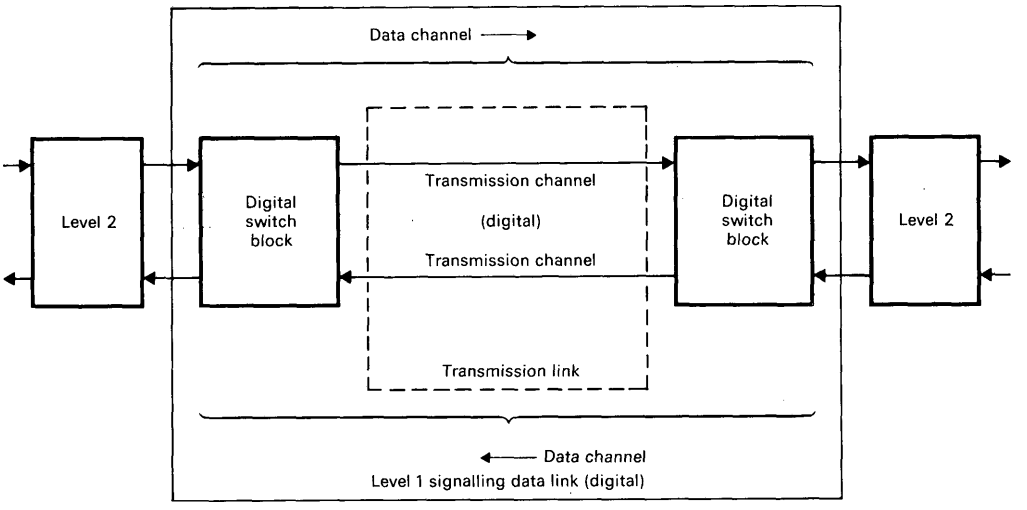
1.3 A digital signalling data link is made up of digital *transmission channels*[1] and digital switches or their terminating equipment providing an interface to signalling terminals. The digital transmission channels may be derived from a digital multiplex signal at 1544, 2048 or 8448 kbit/s having a frame structure as defined in Recommendation G.704 [1], or from digital multiplex streams having a frame structure specified for data circuits (Recommendations X.50 [4], X.51 [5], X.50 *bis* [6], X.51 *bis* [7]).

1.4 An analogue signalling data link is made up of voice-frequency analogue transmission channels either 4 kHz or 3 kHz spaced, and modems.

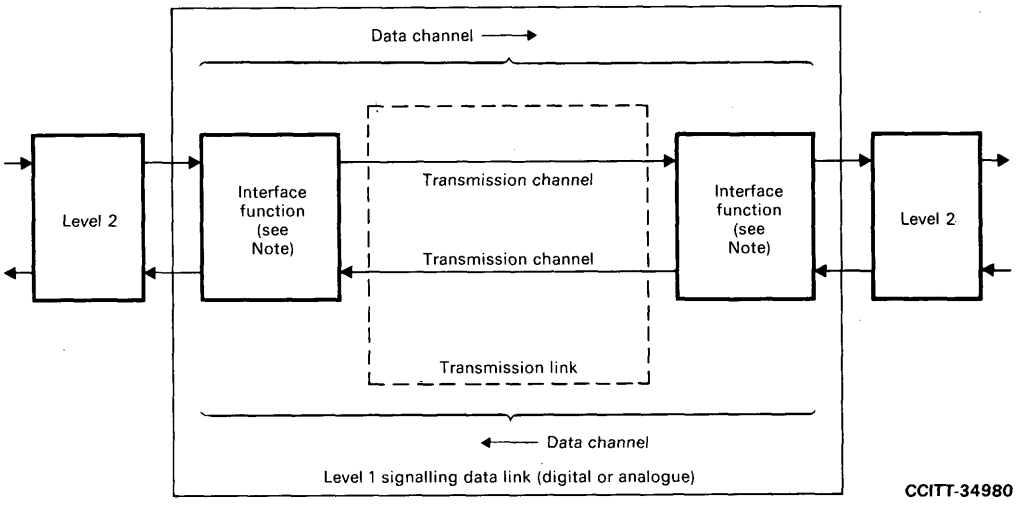
1.5 Signalling System No. 7 is capable of operating over both terrestrial and satellite *transmission links*[1].

---

[1] The terms *transmission channel* and *transmission link* are used in Signalling System No. 7 instead of transfer channel and transfer link used in Signalling System No. 6.




*a) Example 1 – Digital signalling data link via digital switch block*




*Note* – The interface function is provided, for example, by a modem in an analogue signalling data link, a data circuit terminating equipment (DCE) or a time slot access equipment in a digital signalling data link.

*b) Example 2 – Signalling data link (digital or analogue) via interface equipment*

FIGURE 1/Q.702

**Functional configuration of a signalling data link**

1.6 The operational signalling data link shall be exclusively dedicated to the use of a Signalling System No. 7 signalling link between two signalling points. No other information should be carried by the same channel together with the signalling information.

1.7 Equipment such as echo suppressors, digital pads, or A/μ law convertors attached to the transmission link must be disabled in order to assure full duplex operation and bit integrity of the transmitted data stream.

1.8 64-kbit/s digital signalling channels entering a digital exchange via a multiplex structure shall be switchable as semi-permanent channels in the exchange.

## 2 Signalling bit rate

### 2.1 *General*

2.1.1 The standard bit rate on a digital bearer will be 64 kbit/s.

2.1.2 Lower bit rates may be adopted for each application, taking into account the User Part requirements and the capability of available transmission links.

2.1.3 The minimum signalling bit rate for telephone call control applications will be 4.8 kbit/s. For other applications such as network management, bit rates lower than 4.8 kbit/s can also be used.

### 2.2 *Use of bit rates lower than 64 kbit/s*

2.2.1 For national telephone call control applications, use of Signalling System No. 7 at bit rates lower than 64 kbit/s shall take account of the requirement to minimize the answer signal delay when in-band line signalling systems are involved (Recommendation Q.27 [8]).

2.2.2 Signalling System No. 7 can be used for direct international application at bit rates lower than 64 kbit/s between countries which have no in-band line signalling systems in their national extension networks (see § 2.1.3).

2.2.3 The possible use of Signalling System No. 7 at bit rates lower than 64 kbit/s between countries which have in-band line signalling systems in their national extension networks is for further study.

## 3 Error characteristics and availability

Error characteristics and availability requirements will conform to relevant Recommendations (for example, Recommendation G.821 [9] on digital circuits). No additional characteristics or requirements will be specified in this Recommendation.

## 4 Interface specification points

4.1 Interface requirements may be specified at one of three points, A, B or C in Figure 2/Q.702. The appropriate point depends on the nature of transmission links used and the approach toward the implementation of interface equipment adopted by each Administration.

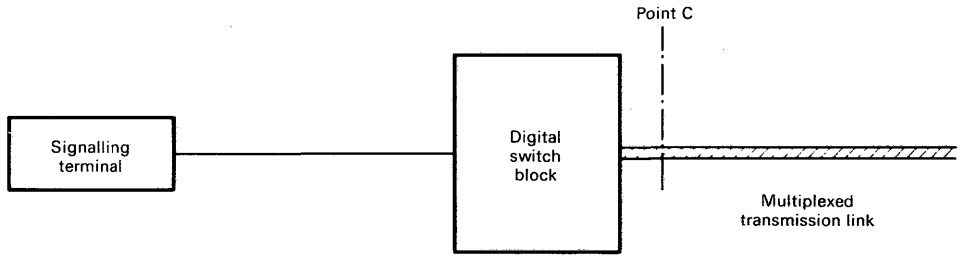
4.2 For the international application, interface requirements at either Point B or Point C will apply.

4.3 Interface requirements for an international digital signalling data link will be specified at Point C in accordance with the specific multiplex structure used (see § 5.)

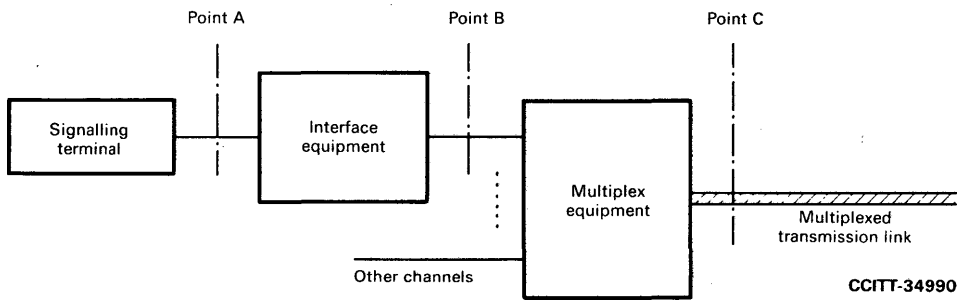
4.4 Interface requirements for an international analogue signalling data link will be specified at Point B on a single channel basis, and thus are independent of multiplex equipment used. (See § 6.)

4.5 Interface at Point A may or may not appear in particular implementations, as each Administration may adopt different approaches towards the implementation of interface equipment. If it does appear in implementations, then the interface requirements specified in Recommendations V.10 [10], V.11 [11], V.24 [12], V.28 [13], V.35 [14], V.36 [15], X.24 [16] and G.703 [17] (for 64-kbit/s interface) should be followed as appropriate.

4.6 Implementations which do not follow all the requirements in the relevant Recommendations cited above should nevertheless take into account those requirements that are specified for testing and maintenance actions which require communication between the two ends of a data link. Interface requirements for testing and maintenance are specified in Recommendation Q.707.




*a) Example 1 – Digital signalling data link via a digital switch block*




*b) Example 2 – Signalling data link (digital or analogue) via interface equipment*

FIGURE 2/Q.702

**Interface specification points**

## 5 Digital signalling data link

### 5.1 *Signalling data link derived from the 2048-kbit/s digital path*

When a signalling data link is to be derived from a 2048-kbit/s digital path, the following shall apply:

a) The interface requirements, specified at Point C in Figure 2/Q.702, should comply with Recommendations G.703 [17] for the electrical characteristics and G.704 [1] for the functional characteristics, in particular the frame structure.

b) The signalling bit rate shall be 64 kbit/s.

c) The standard channel time slot for the use of a signalling data link is time slot 16. When time slot 16 is not available, any channel time slot available for 64-kbit/s user transmission may be used.

d) No bit inversion is performed.

### 5.2 *Signalling data link derived from the 8448-kbit/s digital path*

When a signalling data link is to be derived from a 8448-kbit/s digital link, the following shall apply:

a) The interface requirements, specified at Point C in Figure 2/Q.702, should comply with Recommendations G.703 [23] for the electrical characteristics and G.704 [1] for the functional characteristics, in particular the frame structure.

b) The signalling bit rate shall be 64 kbit/s.

c) The standard channel time slots for the use of a signalling data link are time slots 67 to 70 in descending order of priority. When they are not available, any channel time slot available for 64-kbit/s user transmission may be used.

d) No bit inversion is performed.

5.3 *Signalling data link derived from the 1544-kbit/s digital path*

(For further study.)

*Note* – When a signalling bit rate of 64 kbit/s is adopted, the values of bits should be inverted within the signalling terminal or the interface equipment in order to meet the minimum mark density requirements of the Recommendation G.733 [2] based PCM systems.

5.4 *Signalling data link established over a digital path made up by digital sections based on different digital hierarchies*

When a signalling data link is to be established between networks based on different digital hierarchies and speech encoding laws, the following shall apply:

a) The interface requirements, specified at Point C in Figure 2/Q.702, should comply with Recommendations G.703 [17] for the electrical characteristics and G.802 [3] for other aspects, e.g., for interworking arrangements.

b) The signalling bit rate shall be 64 kbit/s.

c) No bit inversion is performed.

5.5 *Signalling data link established over data circuits*

When a signalling data link is to be established over data circuits derived from a 64-kbit/s digital stream having a frame structure as specified in such Recommendations as X.50 [10], X.51 [11], X.50 *bis* [12] and X.51 *bis* [13] the following shall apply:

a) The interface requirements, specified at Point C in Figure 2/Q.702, should comply with relevant requirements in one of the above-mentioned Recommendations, applicable to the environment of the intended use.

b) When 64-kbit/s multiplexed streams are carried on 2048-kbit/s or 1544-kbit/s digital links, Recommendation G.704 [1], should apply.

## 6 Analogue signalling data link

6.1 *Signalling bit rate*

6.1.1 Applications of the analogue signalling data link must take account of the delay requirements described in § 2.2.

6.1.2 For telephone call control applications, the signalling bit rate over an analogue signalling data link shall be higher or equal to 4.8 kbit/s.

6.2 *Interface requirements*

In case of 4.8-kbit/s operation, interface requirements specified at the interface point B in Figure 2/Q.702 should comply with relevant requirements specified for 4.8-kbit/s modems in Recommendations V.27 [18] and V.27 *bis* [19]. In addition, the following shall apply:

a) Application of either Recommendations V.27 [18] or V.27 *bis* [19] depends on the quality of the analogue transmission channels used. Recommendation V.27 [18] shall apply only to transmission channels conforming to Recommendation M.1020 [20], while Recommendation V.27 *bis* [19] to transmission channels conforming to Recommendation M.1020 [20] or of lower quality.

b) Full duplex operation over a 4-wire transmission link should be adopted.

c) If a separate modem is to be used, the interface requirements specified in Recommendations V.10 [10], V.11 [11], V.24 [12] and V.28 [13], applicable at Point A in Figure 2/Q.702, should be followed as much as possible.

**References**


[1] CCITT Recommendation *Functional characteristics of interfaces associated with network nodes*, Vol. III, Rec. G.704.

[2] CCITT Recommendation *Characteristics of primary PCM multiplex equipment operating at 1544 kbit/s*, Vol. III, Rec. G.733.

[3] CCITT Recommendation *Interconnection of digital paths using different techniques*, Vol. III, Rec. G.802.

[4] CCITT Recommendation *Fundamental parameters of a multiplexing scheme for the international interface between synchronous data networks*, Vol. VIII, Rec. X.50.

[5] CCITT Recommendation *Fundamental parameters of a multiplexing scheme for the international interface between synchronous data networks*, Vol. VIII, Rec. X.51.

[6] CCITT Recommendation *Fundamental parameters of a 48-kbit/s user data signalling rate transmission scheme for the international interface between synchronous data networks*, Vol. VIII, Rec. X.50 *bis*.

[7] CCITT Recommendation *Fundamental parameters of a 48-kbit/s user data signalling rate transmission scheme for the international interface between synchronous data networks using 10-bit envelope structure*, Vol. VIII, Rec. X.51 *bis*.

[8] CCITT Recommendation *Transmission of the answer signal*, Vol. VI, Rec. Q.27.

[9] CCITT Recommendation *Error performance on an international digital connection forming part of an integrated services digital network*, Vol. III, Rec. G.821.

[10] CCITT Recommendation *Electrical characteristics for unbalanced double-current interchange circuits for general use with integrated circuit equipment in the field of data communications*, Vol. VIII, Rec. V.10.

[11] CCITT Recommendation *Electrical characteristics for balanced double-current interchange circuits for general use with integrated circuit equipment in the field of data communications*, Vol. VIII, Rec. V.11.

[12] CCITT Recommendation *List of definitions for interchange circuits between data-terminal equipment and data circuit-terminating equipment*, Vol. VIII, Rec. V.24.

[13] CCITT Recommendation *Electrical characteristics for unbalanced double-current interchange circuits*, Vol. VIII, Rec. V.28.

[14] CCITT Recommendation *Data transmission at 48 kbit/s per second using 60-108 kHz group band circuits*, Vol. VIII, Rec. V.35.

[15] CCITT Recommendation *Modems for synchronous data transmission using 60-108 kHz group band circuits*, Vol. VIII, Rec. V.36.

[16] CCITT Recommendation *List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) on public data networks*, Vol. VIII, Rec. X.24.

[17] CCITT Recommendation *Physical/electrical characteristics of hierarchical digital interfaces*, Vol. III, Rec. G.703.

[18] CCITT Recommendation *4800 bit/s per second modems with manual equalizer standardized for use on leased telephone-type circuits*, Vol. VIII, Rec. V.27.

[19] CCITT Recommendation *4800/2400 bit/s per second modem with automatic equalizer standardized for use on leased telephone-type circuits*, Vol. VIII, Rec. V.27 *bis*.

[20] CCITT Recommendation *Characteristics of special quality international leased circuits with special bandwidth conditioning*, Vol. IV, Rec. M.1020.

**Recommendation Q.703**

## SIGNALLING LINK

## 1 General

### 1.1 *Introduction*

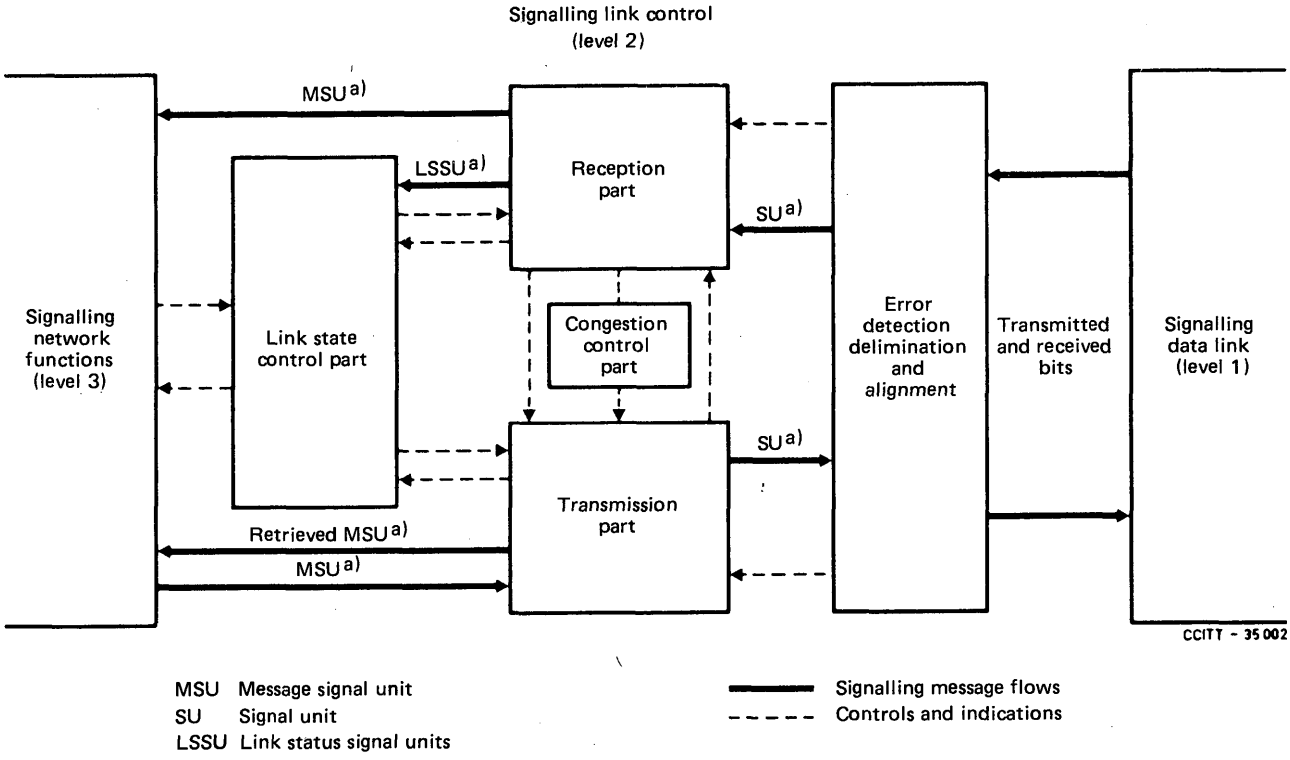
1.1.1 This Recommendation describes the functions and procedures for and relating to the transfer of signalling messages over one signalling data link. The signalling link functions, together with a signalling data link as bearer, provide a signalling link for reliable transfer of signalling messages between two directly connected *signalling points.*

Signalling messages delivered by superior hierarchical levels are transferred over the signalling link in variable length *signal units.* The signal units include transfer control information for proper operation of the signalling link in addition to the signalling information.

1.1.2 The signalling link functions comprise:

a) signal unit delimitation,
b) signal unit alignment,
c) error detection,
d) error correction,
e) initial alignment,
f) signalling link error monitoring,
g) flow control.

All these functions are coordinated by the *link state control* (see Figure 1/Q.703).




a) These signal units do not include all error control information.

FIGURE 1/Q.703

**Interactions of the functional specification blocks for signalling link control**

## 1.2 *Signal unit delimitation and alignment*

The beginning and end of a signal unit are indicated by a unique 8-bit pattern, called the *flag.* Measures are taken to ensure that the pattern cannot be imitated elsewhere in the unit.

Loss of alignment occurs when a bit pattern disallowed by the delimitation procedure (more than six consecutive 1s) is received, or when a certain maximum length of signal unit is exceeded.

Loss of alignment will cause a change in the mode of operation of the *signal unit error rate monitor.*

## 1.3 *Error detection*

The error detection function is performed by means of 16 check bits provided at the end of each signal unit. The check bits are generated by the transmitting signalling link terminal by operating on the preceding bits of the signal unit following a specified algorithm. At the receiving *signalling link terminal*[1)], the received check bits are operated on using specified rules which correspond to that algorithm.

If consistency is not found between the received check bits and the preceding bits of the signal unit, according to the algorithm, then the presence of errors is indicated and the signal unit is discarded.

## 1.4 *Error correction*

1.4.1 Two forms of error correction are provided, the *basic method* and the *preventive cyclic retransmission method.* The following criteria should be used for determining the international fields of application for the two methods:

a) the basic method applies for signalling links using non-intercontinental terrestrial transmission means and for intercontinental signalling links where the one-way propagation delay is less than 15 ms;

b) the preventive cyclic retransmission method applies for intercontinental signalling links where the one-way propagation delay is greater than or equal to 15 ms and for all signalling links established via satellite.

In cases where one signalling link within an international link set is established via satellite, the preventive cyclic retransmission method should be used for all signalling links of that link set.

1.4.2 The basic method is a non-compelled, positive/negative acknowledgement, retransmission error correction system. A signal unit which has been transmitted is retained at the transmitting signalling link terminal until a positive acknowledgement for that signal unit is received. If a negative acknowledgement is received, then the transmission of new signal units is interrupted and those signal units which have been transmitted but not yet positively acknowledged starting with that indicated by the negative acknowledgement will be retransmitted once, in the order in which they were first transmitted.

1.4.3 The preventive cyclic retransmission method is a non-compelled, positive acknowledgement, cyclic retransmission, forward error correction system. A signal unit which has been transmitted is retained at the transmitting signalling link terminal until a positive acknowledgement for that signal unit is received. During the period when there are no new signal units to be transmitted all the signal units which have not yet been positively acknowledged are retransmitted cyclically.

The *forced retransmission procedure* is defined to ensure that forward error correction occurs in adverse conditions (e.g. high error rate and/or high traffic loading).

When a predetermined number of retained, unacknowledged signal units exists, the transmission of new signal units is interrupted and the retained signal units are retransmitted cyclically until the number of unacknowledged signal units is reduced.

---

[1)] A *signalling link terminal* refers to the means of performing all of the functions defined at level 2 regardless of their implementation.

### 1.5 *Initial alignment*

The initial alignment procedure is appropriate to both first time initialization (e.g., after "switch-on") and alignment in association with restoration after a link failure. The procedure is based on the compelled exchange of status information between the two *signalling points* concerned and the provision of a proving period. No other signalling link is involved in the initial alignment of any particular link, the exchange occurs only on the link to be aligned.

### 1.6 *Signalling link error monitoring*

Two signalling link error rate monitor functions are provided; one which is employed whilst a signalling link is in service and which provides one of the criteria for taking the link out of service, and one which is employed whilst a link is in the proving state of the initial alignment procedure. These are called the *signal unit error rate monitor* and the *alignment error rate monitor* respectively. The characteristics of the signal unit error rate monitor are based on a signal unit error count, incremented and decremented using the "leaky bucket" principle whilst the alignment error rate monitor is a linear count of signal unit errors. During loss of alignment, the signal unit error rate monitor error count is incremented in proportion to the period of the loss of alignment.

### 1.7 *Link state control functions*

*Link state control* is a function of the signalling link which provides directives to the other signalling link functions. The interfaces with link state control are shown in Figure 1/Q.703 and Figure 7/Q.703. The split into the functional blocks shown in the figures is made to facilitate description of the signalling link procedures and should not be taken to imply any particular implementation.

The link state control function is shown in the overview diagram, Figure 2/Q.703, and the detailed state transition diagram, Figure 8/Q.703.

### 1.8 *Flow control*

Flow control is initiated when congestion is detected at the receiving end of the signalling link. The congested receiving end of the link notifies the remote transmitting end of the condition by means of an appropriate link status signal unit and it withholds acknowledgements of all incoming message signal units. When congestion abates acknowledgements of all incoming message signal units is resumed. While congestion exists, the remote transmitting end is periodically notified of this condition. The remote transmitting end will indicate the link as failed if the congestion continues too long.

## 2 Basic signal unit format

### 2.1 *General*

Signalling and other information originating from a User Part is transferred over the signalling link by means of signal units.

A signal unit is constituted of a variable length *signalling information field* which carries the information generated by a *User Part* and a number of fixed length fields which carry information required for message transfer control. In the case of link status signal units, the signalling information field and the service information octet is replaced by a status field which is generated by the signalling link terminal.

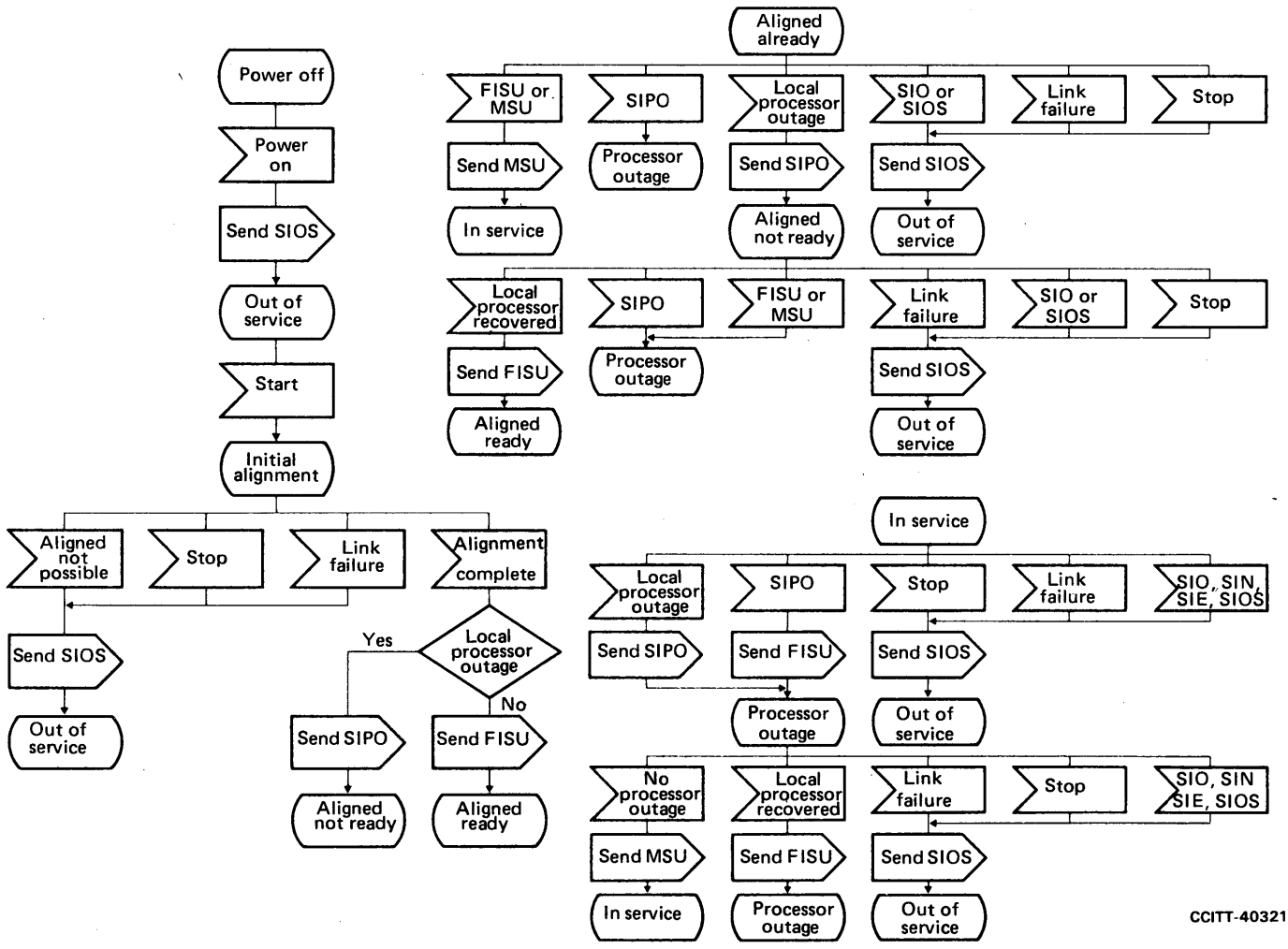
### 2.2 *Signal unit format*

Three types of signal unit are differentiated by means of the *length indicator* contained in all signal units, i.e., message signal units, link status signal units and fill-in signal units. Message signal units are retransmitted in case of error, link status signal unit and fill-in signal units are not. The basic formats of the signal units are shown in Figure 3/Q.703.

## 2.3 *Function and codes of the signal unit fields*

### 2.3.1 *General*

The message transfer control information encompasses 8 fixed length fields in the signal unit which contain information required for error control and message alignment.




FISU Fill-in signal unit
MSU Message signal unit
SIE Status indication "E"
SIN Status indication "N"

SIO Status indication "O"
SIOS Status indication "out of service"
SIPO Status indication "processor outage"

FIGURE 2/Q.703

**Overview diagram of link state control**

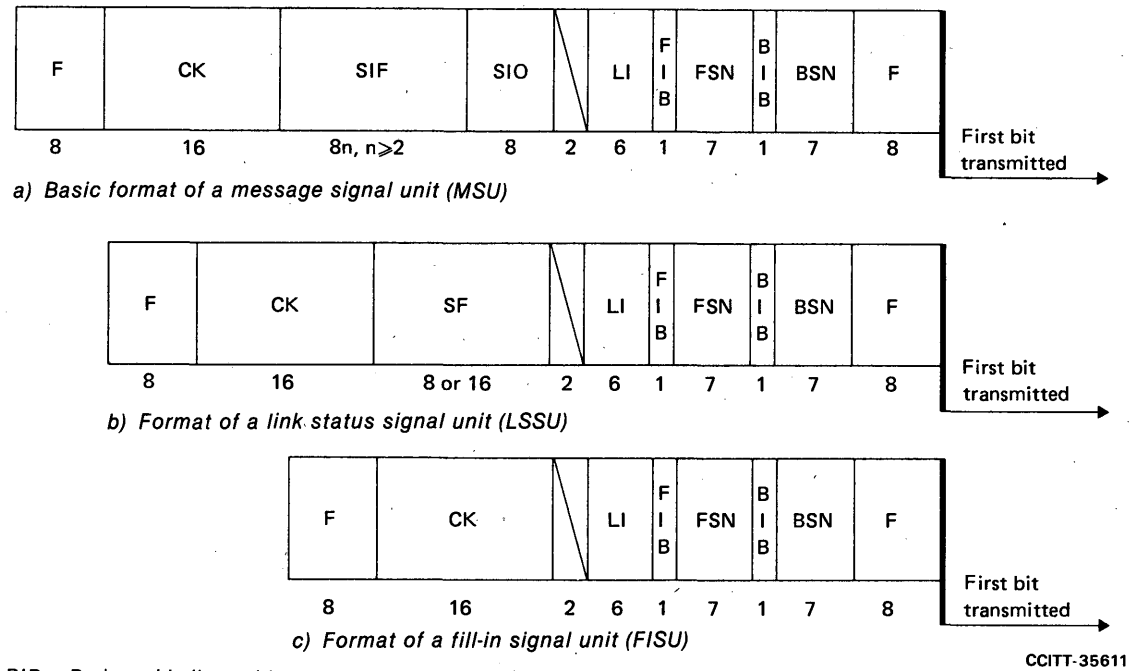



FIGURE 3/Q.703

**Signal unit formats**

2.3.2 *Flag*

The opening flag indicates the start of a signal unit. The opening flag of one signal unit is normally the closing flag of the preceding signal unit. The closing flag indicates the end of a signal unit. The bit pattern for the flag is 01111110.

2.3.3 *Length indicator*

The length indicator is used to indicate the number of octets following the length indicator octet and preceding the *check bits* and is a number in binary code in the range 0-63. The length indicator differentiates between the three types of signal units as follows:

| | |
|---|---|
| Length indicator = 0: | fill in signal unit |
| Length indicator = 1 or 2: | link status signal unit |
| Length indicator > 2: | message signal unit |

In the case that the signalling information field of a message signal unit is spanning 62 octets or more, the length indicator is set to 63.

It is mandatory that LI is set by the transmitting end to its correct value as specified above.

2.3.4 *Service information octet*

The *service information octet* is divided into the *service indicator* and the *subservice field.* The service indicator is used to associate signalling information with a particular user part and is present only in message signal units.

The content of the subservice field is described in Recommendation Q.704, § 14.2.2.

*Note* – The Message Transfer Part may handle messages for different users (i.e., messages with different service indicators) with different priorities. These priorities are for further study.

2.3.5 *Sequence numbering*

The *forward sequence number* is the sequence number of the signal unit in which it is carried.

The *backward sequence number* is the sequence number of a signal unit being acknowledged.

The forward sequence number and backward sequence number are numbers in binary code from a cyclic sequence ranging from 0 to 127 (see §§ 5 and 6).

2.3.6 *Indicator bits*

The *forward indicator bit* and *backward indicator bit* together with the forward sequence number and backward sequence number are used in the basic error control method to perform the signal unit sequence control and acknowledgement functions. (See §§ 5.2 and 6.)

2.3.7 *Check bits*

Every signal unit has 16 check bits for error detection. (See § 4.)

2.3.8 *Signalling information field*

The *signalling information field* consists of an integral number of octets, greater than or equal to 2 and less than or equal to 272.

The value 272 allows a single message signal unit to accommodate information blocks of up to 268 octets in length accompanied by a routing label.

The format and codes of the signalling information field are defined for each user part.

2.3.9 *Status field*

The formats and codes of the *status field* are described in § 11.

2.3.10 *Spare fields*

Spare fields are coded 0, unless otherwise indicated (see Figures 3/Q.703 and 6/Q.703).

2.4 *Order of bit transmission*

Each of the fields mentioned in § 2.3 will be transmitted in the order indicated in Figure 3/Q.703.

Within each field or subfield the bits will be transmitted with the least significant bit first. The 16 check bits are transmitted in the order generated (see § 4).

## 3 Signal unit delimitation

3.1 *Flags*

A signal unit includes an opening flag (see § 2.2). The opening flag of a signal unit is normally considered to be the closing flag of the preceding signal unit (however, see Note to § 5). In certain conditions (e.g., signalling link overload) a limited number of flags may be generated between two consecutive signal units. However, a signalling link terminal always should be able to receive consecutive signal units with one or more multiple flags inserted between them.

3.2 *Zero insertion and deletion*

To ensure that the flag code is not imitated by any other part of the signal unit the transmitting signalling link terminal inserts a 0 after every sequence of five consecutive 1s before the flags are attached and the signal unit is transmitted. At the receiving signalling link terminal, after flag detection and removal, each 0 which directly follows a sequence of five consecutive 1s is deleted.

## 4 Acceptance procedure

### 4.1 *Acceptance of alignment*

4.1.1 A flag which is not followed immediately by another flag is considered an opening flag. Whenever an opening flag is received, the beginning of a signal unit is assumed. When the next flag (a closing flag) is received it is assumed to be the termination of the signal unit.

4.1.2 If seven or more consecutive 1s are received, the signal unit error rate monitor or alignment error rate monitor enters the "octet counting" mode (see § 4.1.4) and the next valid flag is searched for.

4.1.3 After deletion of the 0s inserted for transparency, the received signal unit length is checked for being a multiple of 8 bits and at least 6 octets, including opening flag. If it is not, then the signal unit is discarded and the signal unit error rate monitor or alignment error rate monitor is incremented. If more than $m + 7$ octets are received before a closing flag, the "octet counting" mode is entered (see Figure 11/Q.703) and the signal unit is discarded. $m$ is the maximum length of the signalling information field (in octets) allowed on a signalling link. $m$ takes the value 272. In the case of the basic error control method a negative acknowledgement will be sent, if required, according to the rules set out in § 5.2.

4.1.4 When the "octet counting" mode is entered all the bits received after the last flag and before the next flag are discarded. The "octet counting" mode is left when the next correctly-checking signal unit is received, and this signal unit is accepted.

### 4.2 *Error detection*

The error detection function is performed by means of 16 check bits provided at the end of each signal unit.

The check bits are generated by the transmitting signalling link terminal. They are the ones complement of the sum (modulo 2) of:

i) the remainder of $x^k (x^{15} + x^{14} + x^{13} + x^{12} \ldots + x^2 + x + 1)$ divided (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$, where $k$ is the number of bits in the signal unit existing between, but not including, the final bit of the opening flag and the first bit of the check bits, excluding bits inserted for transparency; and

ii) the remainder after multiplication by $x^{16}$ and then division (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$ of the content of the signal unit existing between, but not including, the final bit of the opening flag and the first bit of the check bits, excluding bits inserted for transparency.

As a typical implementation, at the transmitting signalling link terminal, the initial remainder of the division is preset to all 1s and is then modified by division by the generator polynomial (as described above) on all the fields of the signal unit; the 1s complement of the resulting remainder is transmitted as the 16 check bits.

At the receiving signalling link terminal, the correspondence between the check bits and the remaining part of the signal unit is checked; if a complete correspondence is not found the signal unit is discarded.

As a typical implementation at the receiving signalling link terminal, the initial remainder is preset to all 1s, and the serial incoming protected bits including the check bits (after the bits inserted for transparency are removed) when divided by the generator polynomial will result in a remainder of 0001110100001111 ($x^{15}$ through $x^0$, respectively) in the absence of transmission errors.

## 5 Basic error correction method

### 5.1 *General*

The basic error correction method is a noncompelled method in which correction is performed by retransmission. In normal operation, the method ensures correct transfer of message signal units over the signalling link, in sequence and with no double delivery. As a consequence, no resequencing or eliminating of the received information is required within the user parts.

*Positive acknowledgements* are used to indicate correct transfer of message signal units. *Negative acknowledgements* are used as explicit requests for retransmission of signal units received in a corrupt form.

To minimize the number of retransmissions and the resulting message signal unit delay, a request for retransmission is made only when a message signal unit (not another signal unit) has been lost because of, for example, transmission errors or disturbances.

The method requires that transmitted but not yet positively acknowledged message signal units remain available for retransmission. To maintain the correct message signal unit sequence when a retransmission is made, the message signal unit, the retransmission of which has been requested, and any subsequently transmitted message signal units are retransmitted in the order in which they were originally transmitted.

As part of the error correction method, each signal unit carries a forward sequence number, a *forward indicator bit*, a backward sequence number and a *backward indicator bit*. The error correction procedure operates independently in the two transmission directions. The forward sequence number and forward indicator bit in one direction together with the backward sequence number and backward indicator bit in the other direction are associated with the message signal unit flow in the first direction. They function independently of the message signal unit flow in the other direction and its associated forward sequence number, forward indicator bit, backward sequence number and backward indicator bit.

The transmission of new message signal units is temporarily stopped during retransmissions or when no forward sequence number values are available to be assigned to new message signal units (due to a high momentary load or corruption of positive acknowledgements) (see § 5.2.2).

Under normal conditions, when no message signal units are to be transmitted or retransmitted, fill-in signal units are sent continuously. In some particular cases link status signal units, continuous fill-in signal units or flags may be sent as described in §§ 7, 8 and 11.

## 5.2 *Acknowledgements (positive acknowledgement and negative acknowledgement)*

### 5.2.1 *Sequence numbering*

For the purposes of acknowledgement and signal unit sequence control, each signal unit carries two sequence numbers. The signal unit sequence control is performed by means of the forward sequence number. The acknowledgement function is performed by means of the backward sequence number.

The value of the forward sequence number of a message signal unit is obtained by incrementing (modulo 128, see § 2.3.5) the last assigned value by 1.

This forward sequence number value uniquely identifies the message signal unit until its delivery is accepted without errors, and in correct sequence, by the receiving terminal. The forward sequence number of a signal unit other than a message signal unit assumes the value of the forward sequence number of the last transmitted message signal unit.

### 5.2.2 *Signal unit sequence control*

Information regarding the service information octet, signalling information field, forward sequence number and the length of each message signal unit is retained at the transmitting signalling link terminal until a positive acknowledgement for that signal unit is received (see § 5.2.3). In the meantime the same forward sequence number cannot be used for another message signal unit (see § 5.2.3).

A forward sequence number value can be assigned to a new message signal unit when a positive acknowledgement concerning that value incremented by at least 1 (modulo 128) is received (see § 5.2.3).

This means that not more than 127 message signal units may be available for retransmission.

The action to be taken at the receiving signalling link terminal upon receipt of a correctly checking signal unit is determined by comparison of the received forward sequence number with the forward sequence number of the last previously accepted signal unit, and on comparison of the received forward indicator bit with the latest sent backward indicator bit. In addition, as the appropriate action differs for a message signal unit and another signal unit, the length indicator of the received signal unit must be examined.

a) If the signal unit is a fill-in signal unit then:

i) if the forward sequence number value equals the forward sequence number value of the last accepted message signal unit, the signal unit is processed within the message transfer part;

ii) if the forward sequence number value is different from the forward sequence number of the last accepted message signal unit, the signal unit is processed within the message transfer part. If the received forward indicator bit is in the same state as the last sent backward indicator bit, a negative acknowledgement is sent.

b) If the signal unit is a link status signal unit then it is processed within the message transfer part.

c) If the signal unit is a message signal unit then:

i) if the forward sequence number value is the same as that of the last accepted signal unit, the signal unit is discarded, regardless of the state of the indicator bits;

ii) if the forward sequence number value is one more (modulo 128, see § 2.3.5) than that of the last accepted signal unit and if the received forward indicator bit is in the same state as the last sent backward indicator bit, the signal unit is accepted and delivered to level 3.

Explicit positive acknowledgements to the accepted signal units are sent as specified in § 5.2.3.

If the forward sequence number is one more than that of the last accepted signal unit and if the received forward indicator bit is not in the same state as the last sent backward indicator bit, then the signal unit is discarded;

iii) if the forward sequence number value is different from those values mentioned in (i) and (ii) above, the signal unit is discarded. If the received forward indicator bit is in the same state as the last sent backward indicator bit, a negative acknowledgement is sent.

Processing of the backward sequence number value and backward indicator bit value as described in § 5.3 is performed for message signal units and fill in signal units except when unreasonable backward sequence number value or unreasonable forward indicator bit value is received. Discarding a signal unit means that if it is a message signal unit, it is not delivered to level 3.

### 5.2.3 *Positive acknowledgement*

The receiving signalling link terminal acknowledges the acceptance of one or more message signal units by assigning the forward sequence number value of the latest accepted message signal unit to the backward sequence number of the next signal unit sent in the opposite direction. The backward sequence numbers of subsequent signal units retain this value until a further message signal unit is acknowledged, which will cause a change of the backward sequence number sent.

The acknowledgement to an accepted message signal unit also represents an acknowledgement to all, if any, previously accepted, though not yet acknowledged, message signal units.

### 5.2.4 *Negative acknowledgement*

If a negative acknowledgement is to be sent (see § 5.2.2), then the backward indicator bit value of the signal units transmitted is inverted. The new backward indicator bit value is maintained in subsequently sent signal units until a new negative acknowledgement is to be sent. The backward sequence number assumes the value of the forward sequence number of the last accepted message signal unit.

## 5.3 *Retransmission*

### 5.3.1 *Response to a positive acknowledgement*

The transmitting signalling link terminal examines the backward sequence number value of the received message signal units and fill-in signal units that have satisfied the polynomial error check. The previously sent message signal unit, which has a forward sequence number value identical to the received backward sequence number value, will no longer be available for transmission.

When an acknowledgement of a message signal unit having a given forward sequence number value is received, all other message signal units which preceded that message signal unit are considered to be acknowledged even though the corresponding backward sequence numbers have not been received.

In the case that the same positive acknowledgement is consecutively received a number of times, no further action is taken.

In the case that a message signal unit or fill-in signal unit is received having a backward sequence number value which is not the same as the previous one or one of the forward sequence number values of the signal units available for retransmission, the signal unit is discarded. The following message signal unit or fill-in signal unit is discarded.

If any two backward sequence number values in three consecutively received message signal units or fill-in signal units are not the same as the previous one or any of the forward sequence number values of the signal units in the retransmission buffer at the time that they are received, then level 3 is informed that the link is faulty.

A timing mechanism, timer T7 [2], shall be provided which generates an indication of excessive delay of acknowledgement if, assuming that there are at least one outstanding MSU in the retransmission buffer, no new-acknowledgement has been received within a time-out T7 (see § 12.3). In the case of excessive delay in the reception of acknowledgements a link failure indication is given to level 3.

### 5.3.2 *Response to a negative acknowledgement*

When the received backward indicator bit is not in the same state as the last sent forward indicator bit, all the message signal units available for retransmission are transmitted in correct sequence starting with the signal unit which has a forward sequence number value of one more (modulo 128, see § 2.3.5) than the backward sequence number associated with the received backward indicator bit.

New message signal units can only be sent when the last message signal unit available for retransmission has been transmitted.

At the start of a retransmission the forward indicator bit is inverted, it thus becomes equal to the backward indicator bit value of the received signal units. The new forward indicator bit value is maintained in subsequently transmitted signal units until a new retransmission is started. Thus, under normal conditions the forward indicator bit included in the transmitted signal units is equal to the backward indicator bit value of the received signal units. If a retransmitted message signal unit is lost, then this is detected by a check on the forward sequence number and forward indicator bit (see § 5.2.2) and a new retransmission request is made.

In the case that a message signal unit or a fill-in signal unit is received having a forward indicator bit value indicating the start of a retransmission when no negative acknowledgement has been sent, then that signal unit is discarded. The following message signal unit or fill-in signal unit is discarded.

If any two forward indicator bit values in three consecutively received message signal units or fill-in signal units indicate the start of a retransmission when no negative acknowledgement has been sent at the time that they are received, then level 3 is informed that the link is faulty.

---

[2] Timers defined in Recommendation Q.703 are absolute time values; this means that, due to the possibility to insert multiple flags between signal units (see § 3.1), there may be no fixed relation between the time-out values and the number of signal units transmitted/received during the time-out periods.

### 5.3.3 *Repetition of message signal units*

The signal unit sequence control makes it possible to repeat a message signal unit which has not yet been acknowledged without affecting the basic error correction procedure. Thus a form of forward error correction by means of repetition of message signal units is possible as a national option (e.g., to reduce the effective signalling link speed in special national applications, and in long loop delay applications to lower the retransmission rate and thus reduce the average message delay). In the case of repetition, each signal unit should be defined by its own opening and closing flags (i.e., there should be at least two flags between signal units) to ensure that the repeated signal unit is not lost by the corruption of only a single flag.

## 6 Error correction by preventive cyclic retransmission

### 6.1 *General*

The preventive cyclic retransmission method is essentially a noncompelled forward error correction method, whereby positive acknowledgements are needed to support the forward error correction.

Each message signal unit must be retained at the transmitting signalling link terminal until a positive acknowledgement arrives from the receiving signalling link terminal.

Error correction is effected by preventive cyclic retransmission of the message signal units already sent, though not yet acknowledged. Preventive cyclic retransmission takes place whenever there are no new message signal units or link status signal units available to be sent.

To complement preventive cyclic retransmission, the message signal units available for retransmission are retransmitted with priority when a limit of the number of message signal units or a limit of the number of message signal unit octets available for retransmission has been reached.

Under normal conditions, when no message signal units are to be transmitted or cyclically retransmitted, fill-in signal units are sent. In some particular cases link status signal units, continuous fill-in signal units or flags may be sent as described in §§ 7, 8 and 11.

### 6.2 *Acknowledgements*

#### 6.2.1 *Sequence numbering*

For the purposes of acknowledgement and signal unit sequence control, each signal unit carries 2 sequence numbers. The signal unit sequence control is performed by means of the forward sequence number. The acknowledgement function is performed by means of the backward sequence number.

The value of the forward sequence number of a message signal unit is obtained by incrementing (modulo 128, see § 2.3.5) the last assigned value by 1. This forward sequence number value uniquely identifies the message signal unit until its delivery is accepted without errors and in correct sequence, by the receiving signalling link terminal. The forward sequence number of a signal unit other than a message signal unit assumes the value of the forward sequence number of the last transmitted message signal unit.

#### 6.2.2 *Signal unit sequence control*

Information regarding the service information octet, signalling information field, forward sequence number and the length of each message signal unit is retained at the transmitting signal link terminal until the related acknowledgement for that signal unit is received (see § 6.2.3). In the meantime the same forward sequence number value cannot be used for another message signal unit (see § 6.2.3).

A forward sequence number value can be assigned to a new message signal unit to be sent when a positive acknowledgement concerning that value incremented by at least 1 (modulo 128) is received (see § 6.2.3).

The action to be taken at the receiving signalling link terminal upon receipt of a correctly checking signal unit is determined by comparison of the received forward sequence number with the forward sequence number of the last previously accepted signal unit.

In addition, as the appropriate action differs for a message signal unit and another signal unit, the length indicator of the received signal unit must be examined. The forward indicator bit and the backward indicator bit are not used and are set to 1.

a) If the signal unit is not a message signal unit, then the signal unit is processed within the message transfer part.

b) If the signal unit is a message signal unit then:

   i) if the forward sequence number value is the same as that of the last accepted signal unit, the signal unit is discarded;

   ii) if the forward sequence number value is one more (modulo 128, see § 2.3.5) than that of the last accepted signal unit, the signal unit is accepted and delivered to level 3. Explicit positive acknowledgements for the accepted signal units are sent as specified in § 6.2.3;

   iii) if the forward sequence number value is different from the values mentioned in i) and ii) above, the signal unit is discarded. Processing of the backward sequence number value as described in Section 6.3 is performed for message signal units and fill-in signal units except when unreasonable backward sequence number value is received. Discarding a signal unit means that if it is a message signal unit, it is not delivered to level 3.

### 6.2.3 *Positive acknowledgement*

The receiving signalling link terminal acknowledges the acceptance of one or more message signal units by assigning the forward sequence number value of the latest accepted message signal unit to the backward sequence number of the next signal unit sent. The backward sequence numbers of subsequent signal units retain this value until a further message signal unit is acknowledged, which will cause a change of the backward sequence number sent. The acknowledgement to an accepted message signal unit also represents an acknowledgement to all, if any, previously accepted though not yet acknowledged signal units.

## 6.3 *Preventive cyclic retransmission*

### 6.3.1 *Response to a positive acknowledgement*

All message signal units sent for the first time are retained until they have been positively acknowledged.

The transmitting signalling link terminal examines the backward sequence number value of the received message signal units and fill-in signal units that have satisfied the polynomial error check. The previously sent message signal unit, the forward sequence number value of which is the same as the backward sequence number value, will no longer be available for retransmission.

When an acknowledgement for a message signal unit having a given forward sequence number value is received, all other message signal units, if any, having forward sequence number values preceding that value (modulo 128) are considered to be acknowledged, even though the corresponding backward sequence number has not been received.

In the case that the same positive acknowledgement is consecutively received a number of times, no further action is taken.

In the case that a message signal unit or fill-in signal unit is received having a backward sequence number value which is not the same as the previous one or one of the forward sequence number values of the signal units in the retransmission buffer, the signal unit is discarded. The following message signal unit or fill-in signal unit is discarded.

If any two backward sequence number values in three consecutively received message signal units or fill-in signal units are not the same as the previous one or any of the forward sequence number values of the signal units in the retransmission buffer at the time that they are received, then level 3 is informed that the link is faulty.

A timing mechanism, timer T7, shall be provided which generates an indication of excessive delay of acknowledgement if, assuming that there is at least one outstanding MSU in the retransmission buffer, no new acknowledgement has been received within a time-out T7 (see § 12.3). In the case of excessive delay in the reception of acknowledgements a link failure indications is given to level 3.

6.3.2 *Preventive cyclic retransmission procedure*

i) If no new signal units are available to be sent, the message signal units available for retransmission are retransmitted cyclically.

ii) If new signal units are available, the retransmission cycle, if any, must be interrupted and the signal units be sent with priority.

iii) Under normal conditions, when no message signal units are to be transmitted or cyclically retransmitted, fill-in signal units are sent continuously. In some particular cases link status signal units, continuous fill-in signal units or flags may be sent as described in §§ 7, 8 and 10.

6.4 *Forced retransmission*

To maintain the efficiency of error correction in those cases where automatic error correction by preventive cyclic retransmission alone is made impossible (by, for example, high signalling load), the preventive cyclic retransmission procedures must be complemented by the forced retransmission procedure.

6.4.1 *Forced retransmission procedure*

Both the number of message signal units available for retransmission ($N_1$) and the number of message signal unit octets available for retransmission ($N_2$) are monitored continuously.

If one of them reaches its set limit, no new message signal units or fill-in signal units are sent and the retransmission cycle is continued up to the last message signal unit entered into retransmission buffer with priority, in the order in which they were originally transmitted. If all those message signal units have been sent once and neither $N_1$ nor $N_2$ is at its limit value, the normal preventive cyclic retransmission procedure can be resumed. If not, all the message signal units available for retransmission are sent again with priority.

6.4.2 *Limitation of the values $N_1$ and $N_2$*

$N_1$ is limited by the maximum numbering capacity of the forward sequence number range which dictates that not more than 127 message signal units can be available for retransmission.

In the absence of errors, $N_2$ is limited by the signalling link loop delay $T_L$. It must be ensured that not more than $T_L/T_{eb} + 1$ message signal unit octets are available for retransmission,

where

$T_L$ is the signalling link loop delay, i.e., the time between the sending of a message signal unit and the reception of the acknowledgement for this message signal unit in undisturbed operation; and

$T_{eb}$ is the emission time of one octet.

When some signalling data links of different loop delays are alternated for application to that signalling link, the longest possible signalling link delay may be used to calculate the value of *TL*.

## 7 Initial alignment procedure

7.1 *General*

The procedure is applicable to activation and to restoration of the link. The procedure provides a "normal" proving period for "normal" initial alignment and an "emergency" proving period for "emergency" initial alignment. The decision to apply either the "normal" or the "emergency" procedures is made unilaterally at level 3 (see Recommendation Q.704). Only the signalling link to be aligned is involved in the initial alignment procedure (i.e., no transfer of alignment information over other signalling links is required).

7.2 *Initial alignment status indications*

The initial alignment procedure employs four different alignment status indications:

- status indication "O": out of alignment;
- status indication "N": "normal" alignment status;
- status indication "E": "emergency" alignment status;
- status indication "OS": out of service.

These indications are carried in the status field of the link status signal units (see § 2.2).

Status indication "O" is transmitted when initial alignment has been started and none of the status indications "O", "N" or "E" are received from the link. Status indication "N" is transmitted when, after having started initial alignment, status indication "O", "N" or "E" is received and the terminal is in the "normal" alignment status. Status indication "E" is transmitted when, after having started initial alignment, status indication "O", "N" or "E" is received and the terminal is in the "emergency" alignment status, i.e., it must employ the short "emergency" proving period.

Status indications "N" and "E" indicate the status of the transmitting signalling link terminal; this is not changed by reception of status indications indicating a different status at the remote signalling link terminal. Hence, if a signalling link terminal with a "normal" alignment status receives a status indication "E" it continues to send status indication "N" but initiates the short "emergency" proving period.

Status indication "OS" informs the remote signalling link terminal that for reasons other than processor outage (e.g., link failure) the signalling link terminal can neither receive nor transmit message signal units. Status indication OS is sent on completion of "power on" (see Figures 2/Q.703 and 8/Q.703) until initial alignment is started.

### 7.3 *Initial alignment procedure*

The alignment procedure passes through a number of states during the initial alignment:

- State Idle: the procedure is suspended.
- State "not aligned": the signalling link is not aligned and the terminal is sending status indication "O". Time-out T2[3] is started on entry to State and stopped when State is left[4].
- State "aligned": the signalling link is aligned and the terminal is sending status indication "N" or "E", status indications "N", "E" or "OS" are not received. Time-out T3[3] is started on entry to State and stopped when State is left.
- State 03, "proving"; the signalling link terminal is sending status indication "N" or "E", status indication "O" or "OS" are not received, proving has been started.

  Proving is the means by which the signalling link terminal validates the link's ability to carry signal units correctly by inspecting the signal units. «Proving» must last for a period of T4 before the link can enter the «aligned ready» link state. Expiry of timer T4 (see § 12.3) indicates a successful proving period unless the proving period has been previously aborted up to four times.
- Following successful alignment and proving procedure, the signalling terminal enters Aligned Ready state and the aligned ready time-out T1 is stopped on entry in the In service state and the duration of time-out T1 should be chosen such that the remote end can perform four additional proving attempts.

The procedure itself is described in the overview diagram, Figure 4/Q.703, and in state transition diagram, Figure 9/Q.703.

### 7.4 *Proving periods*

The nominal values of the proving periods are:

$$P_n = 2^{16} \text{ octets transmission time}$$

$$P_e = 2^{12} \text{ octets transmission time}$$

for both 64 kbit/s and lower bit rates. For the corresponding timer T4 values (proving periods), see § 12.3.

---

[3] Timers defined in Recommendation Q.703 are absolute time values; this means that, due to the possibility to insert multiple flags between signal units (see § 3.1), there may be no fixed relation between the time-out values and the number of signal units transmitted/received during the time-out periods.

[4] "If automatic allocation of signalling terminals or signalling data links is applied at both ends of a signalling link, it must be ensured that the values of this time-out are different at each end of a signalling link (see Recommendation Q.704, § 12). In this case T2 low (see § 12.3) is allocated to the signalling point with the lower point code and T2 high to the signalling point with the higher point code. In all other cases, the value of time-out T2 can be the same at both ends of the link.

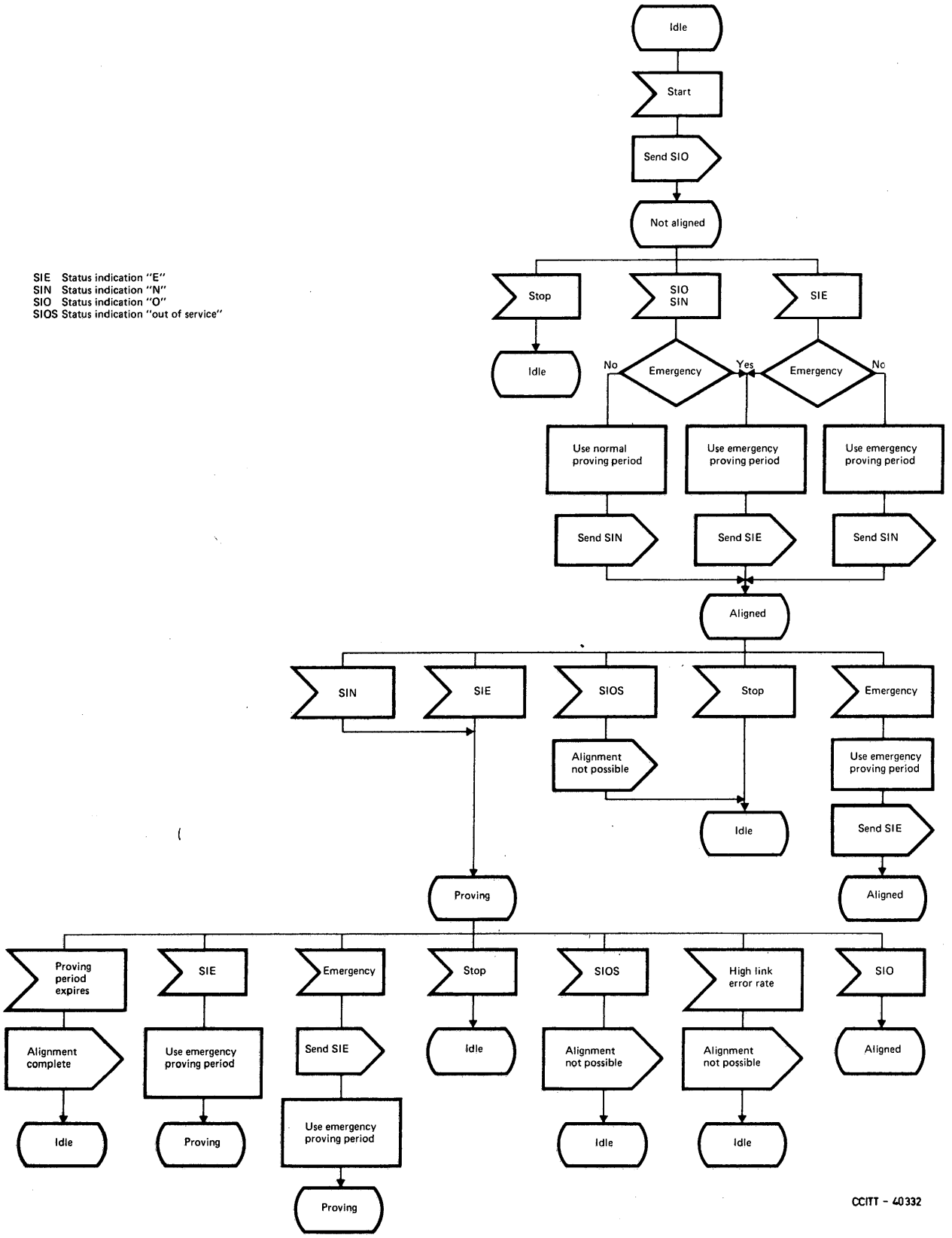



FIGURE 4/Q.703

**Overview diagram of initial alignment control**

## 8 Processor outage

The procedure for dealing with local and/or remote processor outage is described in Figure 10/Q.703.

A processor outage situation occurs when, due to factors at a functional level higher than level 2, use of the link is precluded.

In this context, processor outage refers to a situation when signalling messages cannot be transferred to functional levels 3 and/or 4. This may be because of, for example, a central processor failure. A processor outage condition may not necessarily affect all signalling links in a signalling point, nor does it exclude the possibility that level 3 is able to control the operation of the signalling link.

When level 2 identifies a local processor outage condition, either by receiving an explicit indication from level 3, (i.e., local signalling link blocking, see Recommendation Q.704, § 3.2.6), or by recognizing a failure of level 3, it transmits link status signal units indicating processor outage and discards message signal units received. Provided that the level 2 function at the far end of the signalling link is in its normal operating stage (i.e., transmitting message signal units or fill-in signal units), upon receiving link status signal units indicating processor outage, it notifies level 3 and begins to continuously transmit fill-in signal units.

When the local processor outage condition ceases, normal transmission of message signal units and fill-in signal units is resumed (provided that no local processor outage condition has arisen also at the remote end); as soon as the level 2 function at the remote end correctly receives a message signal unit or fill-in signal unit, it notifies level 3 and returns to normal operation.

Format and code of link status signal units indicating processor outage (status indication "PO") appear in § 11.

## 9 Level 2 flow control

### 9.1 *General*

The procedure is used to handle a level 2 congestion situation. After the congestion is detected at the receiving end of the signalling link, both positive and negative acknowledgements to message units are withheld and a status indication "B" (Busy) is sent from the receiving end of the link to the remote end in order to enable the remote transmitting end to distinguish between congestion and failure situations.

This indication is carried in the status field of a link status signal unit.

*Note* – The receiving end continues to process BSN and BIB carried in signal units received in order to avoid, as far as possible, disturbance of the message flow in the opposite direction and in addition may continue to accept message signal units.

### 9.2 *Detection of congestion*

The mechanism for detecting congestion at the receiving end of a signalling link is implementation dependent and not to be specified.

### 9.3 *Procedure in the congestion situation*

The receiving end of a signalling link which detected a congestion situation, periodically returns a link status signal unit containing a status indication "B" to the remote transmitting end of the link at interval T5 (see § 12.3).

The receiving level 2 also withholds acknowledgement of the message signal unit, which triggered off the congestion detection, and of message signal units received during the congestion situation; that is fill-in signal units or message signal units are sent as usual, but with the backward sequence number and backward indicator bit assigned the values which are contained in the last transmitted signal unit before the congestion is recognized.

At the remote end of the signalling link, every reception of a link status signal unit containing indication "B" causes the excessive delay of acknowledgement timer T7 to be restarted. In addition first reception of the link status signal unit containing a status indication "B" starts a longer supervision timer T6 (see § 12.3). Should timer T6 expire, link failure indication is generated.

9.4 *Congestion abatement procedure*

When congestion abates at the receiving end of the signalling link, transmission of link status signal unit containing a status indication "B" is stopped and normal operation resumed.

At the remote end, the supervision timer T6 is stopped when a negative or positive acknowledgement whose backward sequence number acknowledges a message signal unit in the retransmission buffer is received in case of the basic error correction method, or a positive acknowledgement in case of the PCR method.

*Note* – Congestion onset and abatement detection is an implementation dependent function. Sufficient hysteresis should be provided in the implementation to prevent excessive oscillation between congested and non-congested states.

## 10 Signalling link error monitoring

10.1 *General*

Two link error rate monitor functions are provided; one which is employed whilst a signalling link is in service and which provides one of the criteria for taking the link out of service, and one which is employed whilst a link is in the proving state of the initial alignment procedure (see § 7.3). These are called the signal unit error rate monitor and the alignment error rate monitor respectively.

10.2 *Signal unit error rate monitor*

10.2.1 The signal unit error rate monitor has as its function the estimation of the signal unit error rate in order to decide about the signalling link fault condition. The signal units in error are those rejected by the acceptance procedure (see § 4). The three parameters which determine the signal unit error rate monitor are: the number $T$ (signal units), of consecutive signal units received in error that will cause an error rate high indication to level 3, the lowest signal unit error rate $1/D$ (signal unit errors/signal unit) which will ultimately cause an error rate high indication to level 3, and the number $N$ (octets) of octets that causes an increment of the counter while in the "octet counting" mode. See Figure 5/Q.703.

10.2.2 The signal unit error rate monitor may be implemented in the form of an up/down counter decremented at a fixed rate (for every $D$ received signal units or signal unit errors indicated by the acceptance procedure), but not below zero, and incremented every time a signal unit error is detected by the signal unit acceptance procedure (see § 4), but not above the threshold [$T$ (signal units)]. An excessive error rate will be indicated whenever the threshold $T$ is reached.

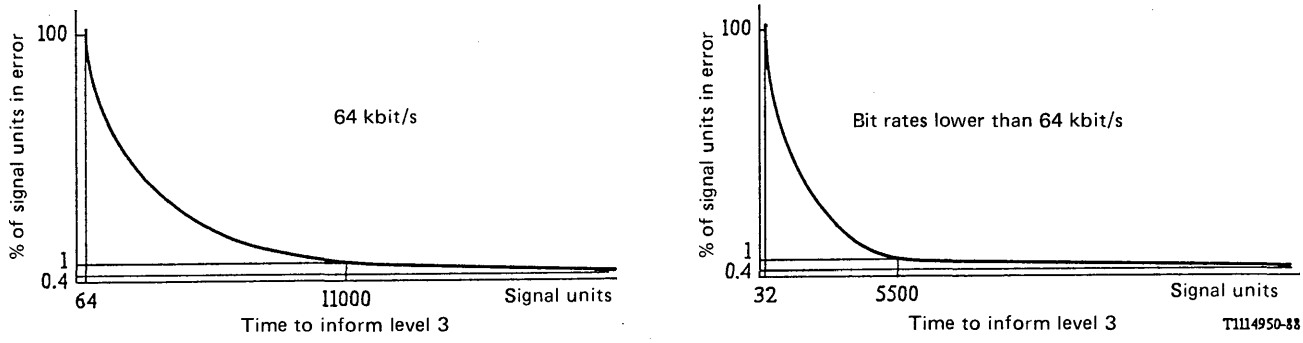



FIGURE 5/Q.703

**Relationship between the expected number of signal units to fault indication and signal units errors rate**

10.2.3 In the "octet counting" mode (see § 4.1) the counter is incremented for every $N$ octets received until a correctly-checking signal unit is detected (causing the "octet counting" mode to be left).

10.2.4 When the link is brought into service the monitor count should start from zero.

10.2.5 The values of the three parameters are:

| | | |
|---|---|---|
| $T$ = 64 signal units<br>$D$ = 256 signal units/signal unit error<br>$N$ = 16 octets | | For 64 kbit/s |
| $T$ = 32 signal units<br>$D$ = 256 signal units/signal unit error<br>$N$ = 16 octets | | For lower bit rates |

In the case of loss of alignment, these figures will give times of approximately 128 ms and 854 ms to initiate changeover for 64 kbit/s and 4.8 kbit/s respectively.

10.2.6 In the case where only random signal unit errors occur over the signalling link, the relationship between the expected number of signal units until threshold of $T$ (signal units) is reached and the signal unit errors rate (signal unit errors/signal units) can be established. This relationship may be expressed by an orthogonal hyperbola which has parameters ($T$, $1/D$). See Figure 5/Q.703.

### 10.3 *Alignment error rate monitor*

10.3.1 The alignment error rate monitor is a linear counter which is operated during normal and emergency proving periods.

10.3.2 The counter is started from zero whenever the proving state (Figure 9/Q.703) of the alignment procedure is entered and is then incremented for every signal unit error detected, if not in the octet counting mode. It is also incremented for every $N$ octets received while in the octet counting mode, as described in § 9.2.3.

10.3.3 When the counter reaches a threshold $T_i$, that particular proving period is aborted; on receipt of a correct signal unit or the expiry of the aborted proving period the proving state is reentered. If proving is aborted $M$ times, the link is returned to the out-of-service state. A threshold is defined for each of the two types of proving period (normal and emergency, see § 7). These are $T_{in}$ and $T_{ie}$ and apply to the normal proving period and the emergency proving period respectively.

Proving is successfully completed when a proving period expires without an excessive error rate being detected and without the receipt of status indication "O" or "OS".

10.3.4 The values of the four parameters for both 64 kbit/s and lower bit rates are:

$T_{in}$ = 4

$T_{ie}$ = 1

$M$ = 5

$N$ = 16

*Note* – It is noted that the emergency proving period may be successfully completed with some probability with a marginal and degraded bit error rate, i.e., around one error in $10^4$ bits – subsequently, the SUERM will quickly indicate an excessive error rate. However, short term operation on a degraded link may be acceptable (e.g., to send management messages).

## 11 Level 2 codes and priorities

### 11.1 *Link status signal unit*

11.1.1 The link status signal unit is identified by a length indicator value equal to 1 or 2. If the length indicator has a value of 1 then the status field consists of one octet; if the length indicator has a value of 2 then the status field consists of two octets.

11.1.2 The format of the one octet status field is shown in Figure 6/Q.703.

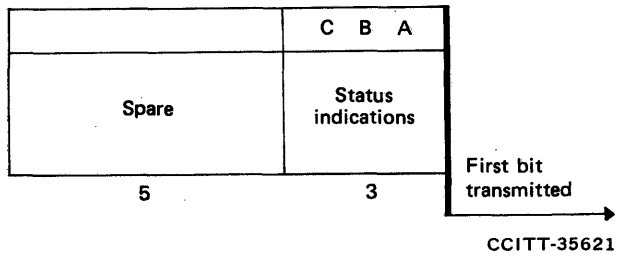



FIGURE 6/Q.703

**Status field format**

When a terminal, which is able to process only a one octet status field, receives a link status signal unit with a two octet status field, the terminal shall ignore the second octet for compatibility reasons but process the first octet as specified.

11.1.3 The use of the link status indications is described in § 7; they are coded as follows:

C B A

0 0 0 – Status indication "O"

0 0 1 – Status indication "N"

0 1 0 – Status indication "E"

0 1 1 – Status indication "OS"

1 0 0 – Status indication "PO"

1 0 1 – Status indication "B"

The spare bits should be ignored at the receiving side.

*Note* – For the use of spare bit D in the national option for a SIF compatibility mechanism, see Recommendation Q.701, § 7.2.6.

11.2 *Transmission priorities within level 2*

11.2.1 Five different items can be transmitted:

i) new message signal units;

ii) message signal units which have not yet been acknowledged;

iii) link status signal units;

iv) fill-in signal units;

v) flags.

In certain failure conditions, it may only be possible to send flags or nothing at all.

11.2.2 For the basic error control method the priorities are:

Highest 1. Link status signal units.

2. Message signal units which have not yet been acknowledged and for which a negative acknowledgement has been received.

3. New message signal units.

4. Fill-in signal units.

Lowest 5. Flags.

11.2.3 For the preventive cyclic retransmission method, the priorities are:

Highest 1. Link status signal units.

2. Message signal units which have not yet been acknowledged and which are stored in a retransmission buffer and exceed one of the parameters $N_1$ and $N_2$.

3. New message signal units.

4. Message signal units which have not yet been acknowledged.

5. Fill-in signal units.

Lowest 6. Flags.

*Note* – In the basic error control method, where the repetition of message signal units is employed as a national option, the repeated message signal unit will have a priority immediately below that of link status signal units.

## 12 State transition diagrams and timers

12.1 Section 12 contains the description of the signalling link control functions, described in this Recommendation, in the form of state transition diagrams according to the CCITT Specification and Description Language (SDL). The following list summarizes these diagrams:

- Level 2 – Functional block diagram: Figure 7/Q.703.
- Link state control: Figure 8/Q.703.
- Initial alignment control: Figure 9/Q.703.
- Processor outage control: Figure 10/Q.703.
- Delimitation, alignment and error detection (receiving): Figure 11/Q.703.
- Delimitation, alignment and error detection (transmitting): Figure 12/Q.703.
- Basic transmission control: Figure 13/Q.703.
- Basic reception control: Figure 14/Q.703.
- Preventive cyclic retransmission transmission control: Figure 15/Q.703.
- Preventive cyclic retransmission reception control: Figure 16/Q.703.
- Alignment error rate monitor: Figure 17/Q.703.
- Signal unit error rate monitor: Figure 18/Q.703.
- Congestion control part: Figure 19/Q.703.

The detailed functional breakdown shown in the following diagrams is intended to illustrate a reference model and to assist interpretation of the text in the earlier sections. The state transition diagrams are intended to show precisely the behaviour of the signalling system under normal and abnormal conditions as viewed from a remote location. It must be emphasized that the functional partitioning shown in the following diagrams is used only to facilitate understanding of the system behaviour and is not intended to specify the functional partitioning to be adopted in a practical implementation of the signalling system.

In the following figures the term *signal unit* refers to units which do not contain all error control information.

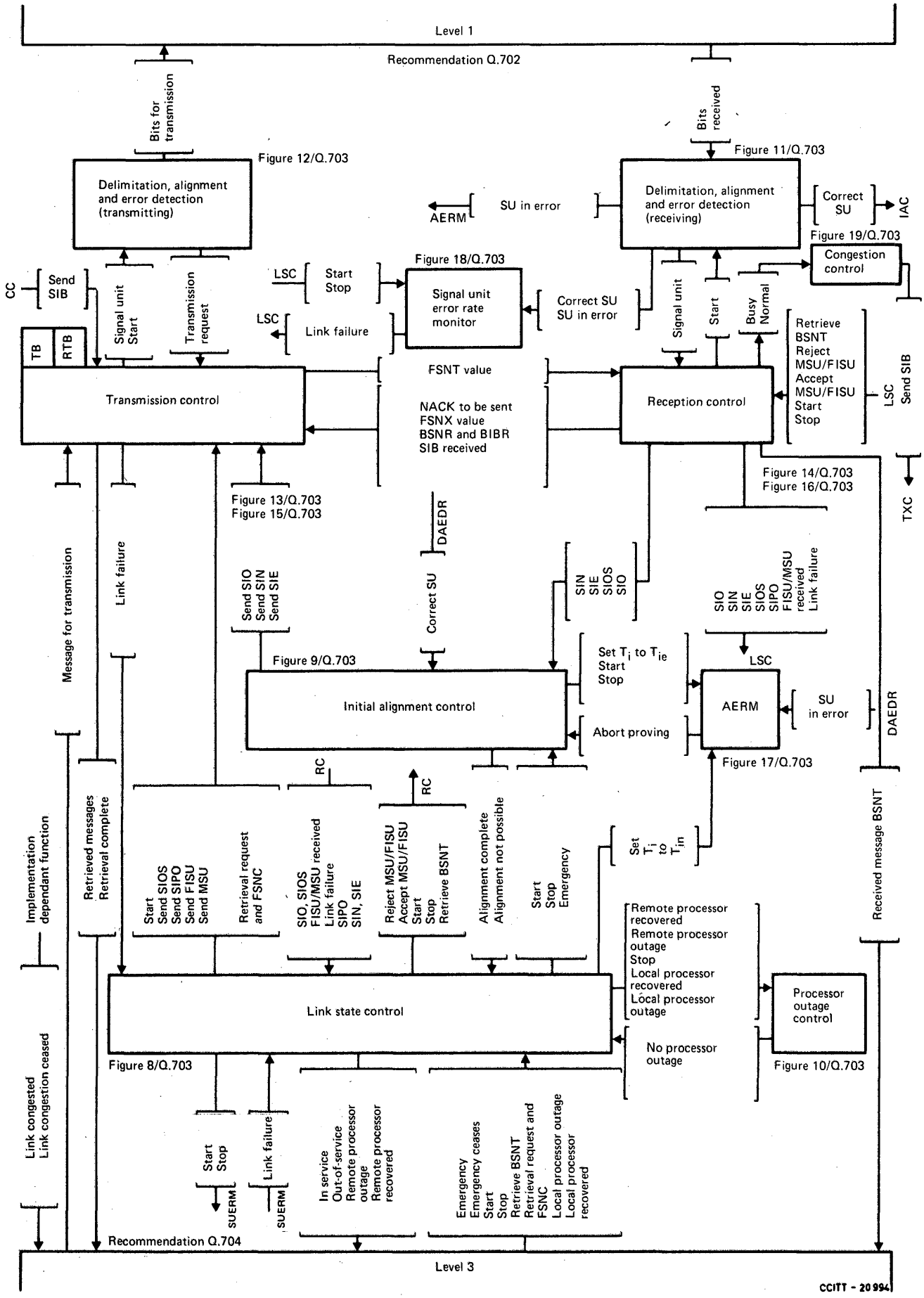
12.2 *Abbreviations*

| | |
|---|---|
| AERM | Alignment error rate monitor |
| BIB | Backward indicator bit |
| BIBR | BIB received |
| BIBT | BIB to be transmitted |
| BIBX | BIB expected |
| BSN | Backward sequence number |
| BSNR | BSN received |
| BSNT | BSN to be transmitted |
| $C_p$ | Count of aborted proving attempts [Figure 9/Q.703 (sheets 2 of 3 and 3 of 3)] |
| $C_m$ | Counter of MSU in TD [Figure 13/Q.703 (sheet 1 of 2) and Figure 15/Q.703 (sheet 1 of 3)] |
| $C_a$ | AERM count (Figure 17/Q.703) |
| $C_s$ | SUERM count (Figure 18/Q.703) |
| CC | Congestion control |

| | |
|---|---|
| DAEDR | Delimitation, alignment and error detection (receiving) |
| DAEDT | Delimitation, alignment and error detection (transmitting) |
| FIB | Forward indicator bit |
| FIBR | FIB received |
| FIBT | FIB transmitted |
| FIBX | FIB expected |
| FISU | Fill-in signal unit |
| FSN | Forward sequence number |
| FSNC | Forward sequence number of last message signal unit accepted by remote level 2 |
| FSNF | FSN of the oldest MSU in the RTB |
| FSNL | FSN of the last MSU in the RTB |
| FSNR | FSN received |
| FSNT | FSN of the last MSU transmitted |
| FSNX | FSN expected |
| IAC | Initial alignment control |
| L2 | Level 2 |
| L3 | Level 3 |
| LSC | Link state control |
| LSSU | Link status signal unit |
| MGMT | Management system – Unspecified implementation dependent management function |
| MSU | Message signal unit |
| M | Maximum length of the SiF in the MSU |
| NSU | Correct SU count |
| NACK | Negative acknowledgement |
| $N_1$ | Maximum number of MSU which are available for retransmission (fixed by the numbering capacity of the FSN) |
| $N_2$ | Maximum number of MSU octets which are available for retransmission (fixed by the common channel loop delay time) |
| POC | Processor outage control |
| RC | Reception control |
| RTB | Retransmission buffer |
| RTR | If = 1 means retransmission expected |
| SIB | Status indication "B" ("Busy") |
| SIE | Status indication "E" ("emergency alignment") |
| SIN | Status indication "N" ("normal alignment") |
| SIO | Status indication "O" ("out of alignment") |
| SIOS | Status indication "OS" ("out of service") |
| SIPO | Status indication "PO" ("processor outage") |
| SU | Signal unit |
| SUERM | Signal unit error rate monitor |
| T | SUERM threshold |
| TB | Transmission buffer |
| TXC | Transmission control |
| UNB | Counter of unreasonable BSN |
| UNF | Counter of unreasonable FIB |
| $T_i$ | AERM threshold |
| $T_{ie}$ | Emergency AERM threshold |
| $T_{in}$ | Normal AERM threshold |
| Z | Pointer to sequence number of next MSU to be retransmitted in transmission code |

12.3 *Timers*

| | |
|---|---|
| T1 | Timer "alignment ready" |
| T1 (64) = 40-50 s | bit rate of 64 kbit/s |
| T1 (4.8) = 500-600 s | bit rate of 4.8 kbit/s |
| T2 = 5-150 s | Timer "not aligned" |
| T2 low = 5-50 s | only for automatic allocation of |
| T2 high = 70-150 s | signalling data links and terminals |
| T3 = 1-1.5 s | Timer "aligned" |
| T4 | Proving period timer = $2^{16}$ or $2^{12}$ octet transmission time |
| T4n (64) = 7.5-9.5 s | normal proving period at 64 kbit/s |
| nominal value 8.2 s | (corresponding to $P_n = 2^{16}$) |
| T4n (4.8) = 100-120 s | nominal proving period at 4.8 kbit/s |
| Nominal value 110 s | (corresponding to $P_n = 2^{16}$) |
| T4e (64) = 400-600 ms | emergency proving period at 64 kbit/s |
| Nominal value 500 ms | (corresponding to $P_e = 12^{12}$) |
| T4e (4.8) = 6-8 s | emergency proving period at 4.8 kbit/s |
| Nominal value 7 s | (corresponding to $P_e = 2^{12}$) |
| T5 = 80-120 ms | Timer "sending SIB" |
| T6 | Timer "remote congestion" |
| T6 (64) = 3-6 s | bit rate of 64 kbit/s |
| T6 (4.8) = 8-12 s | bit rate of 4.8 kbit/s |
| T7 | Timer "excessive delay of acknowledgement" |
| T7 (64) = 0.5-2 s | bit rate of 64 kbit/s |
| For PCR method, | values less than 0.8s should not be used |
| T7 (4.8) = 4-6 s | bit rate of 4.8 kbit/s |
| $P_e$ | Emergency proving period |
| $P_n$ | Normal proving period |

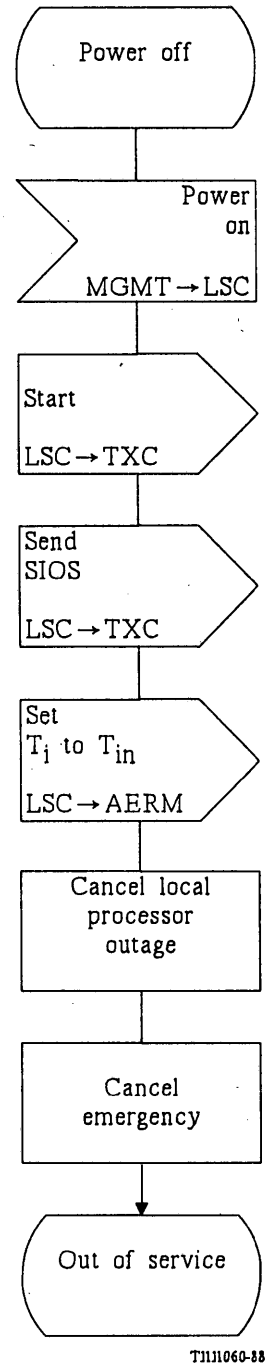



*Note 1* – Abbreviated message names have been used in this diagram (i.e. origin – destination codes are omitted).

*Note 2* – See the abbreviations and timers used in this figure in § 12.

FIGURE 7/Q.703

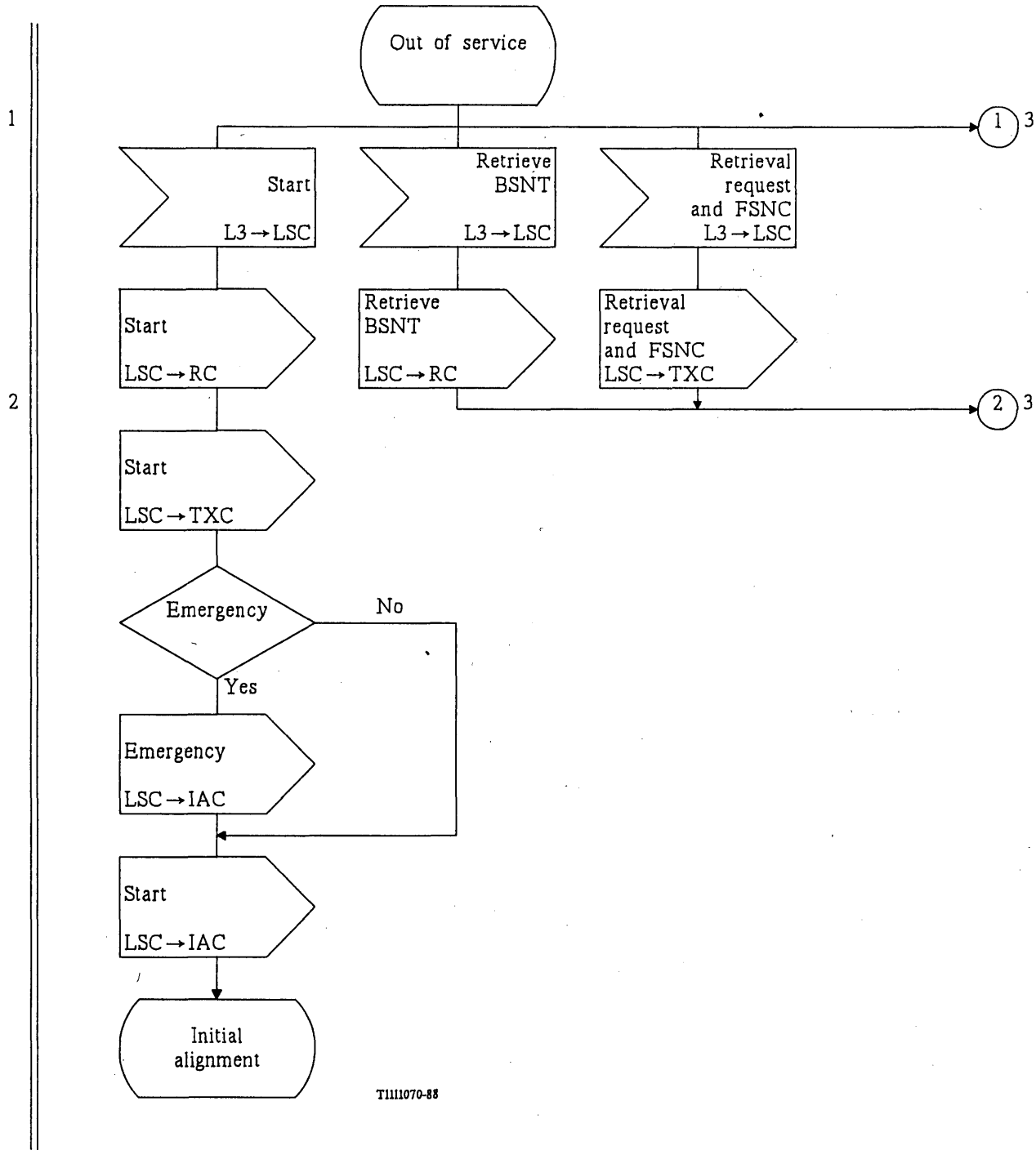
**Level 2 – Functional block diagram**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 1 of 14)

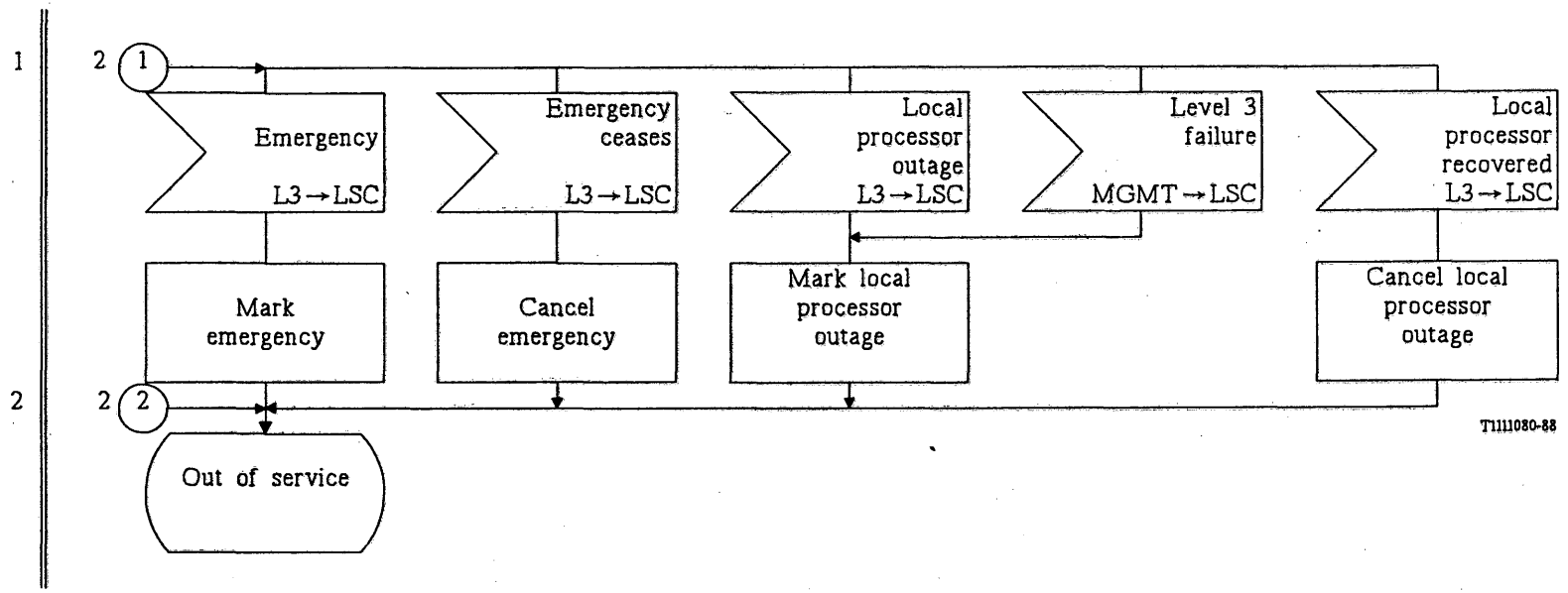
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 2 of 14)

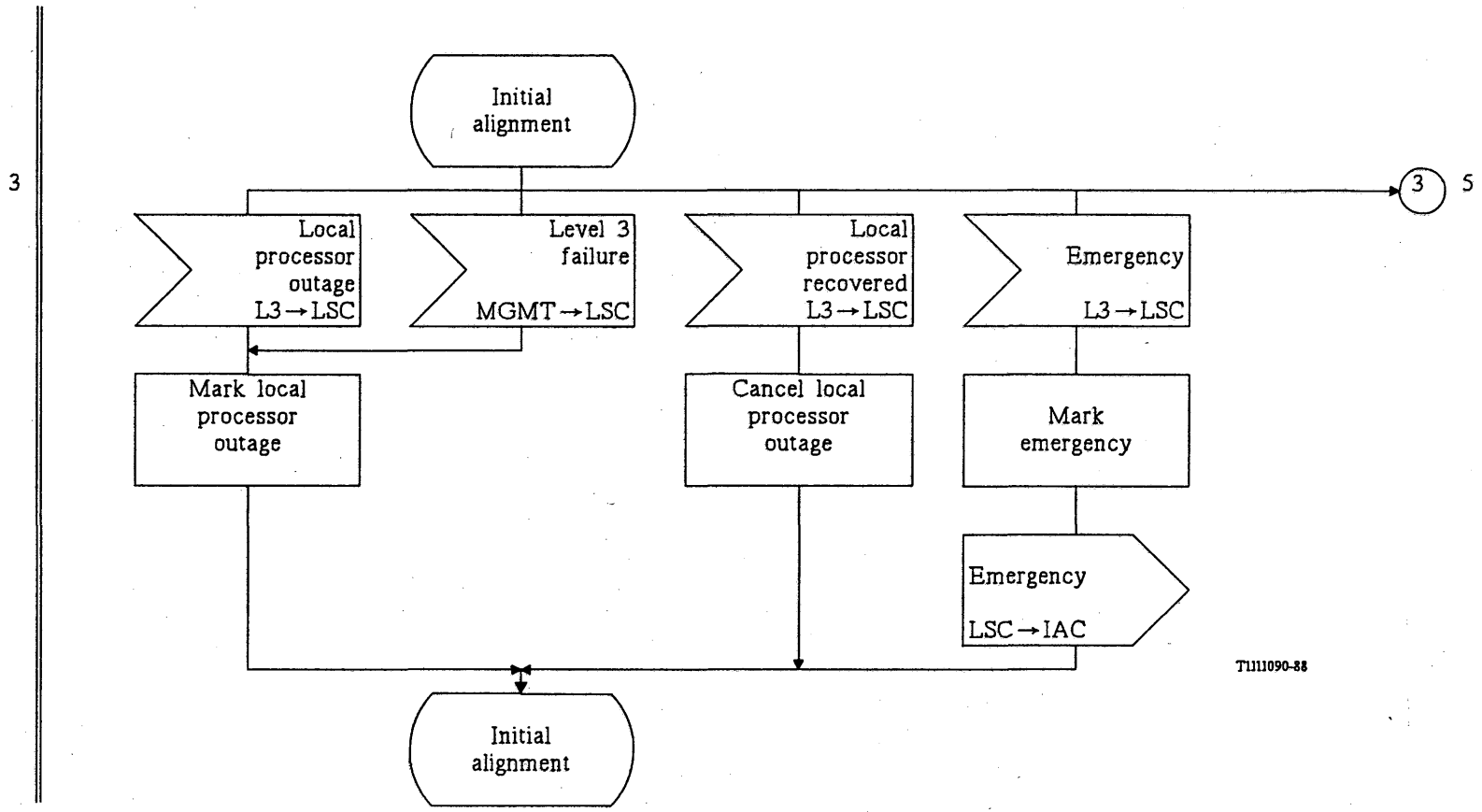
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 3 of 14)

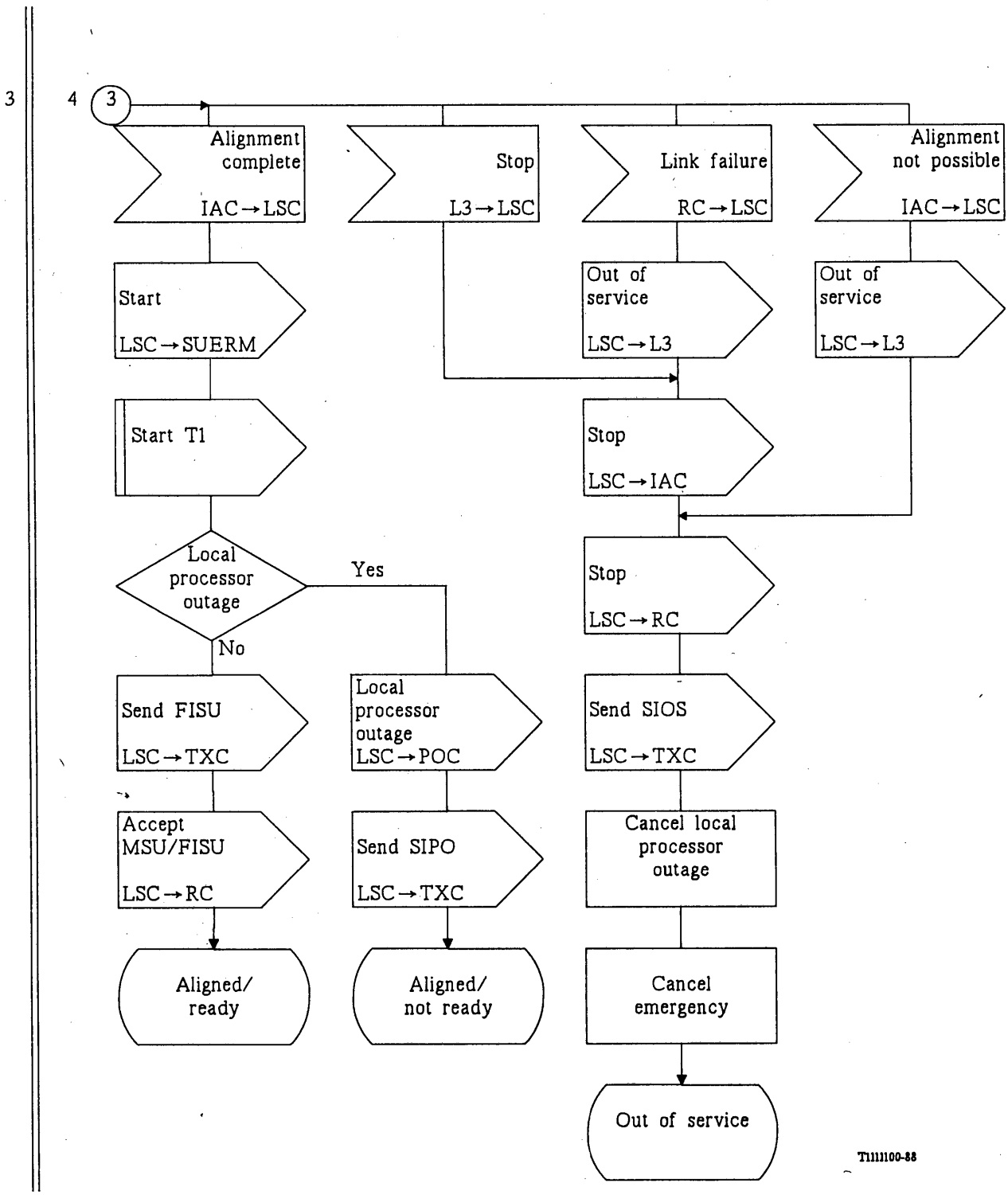
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 4 of 14)

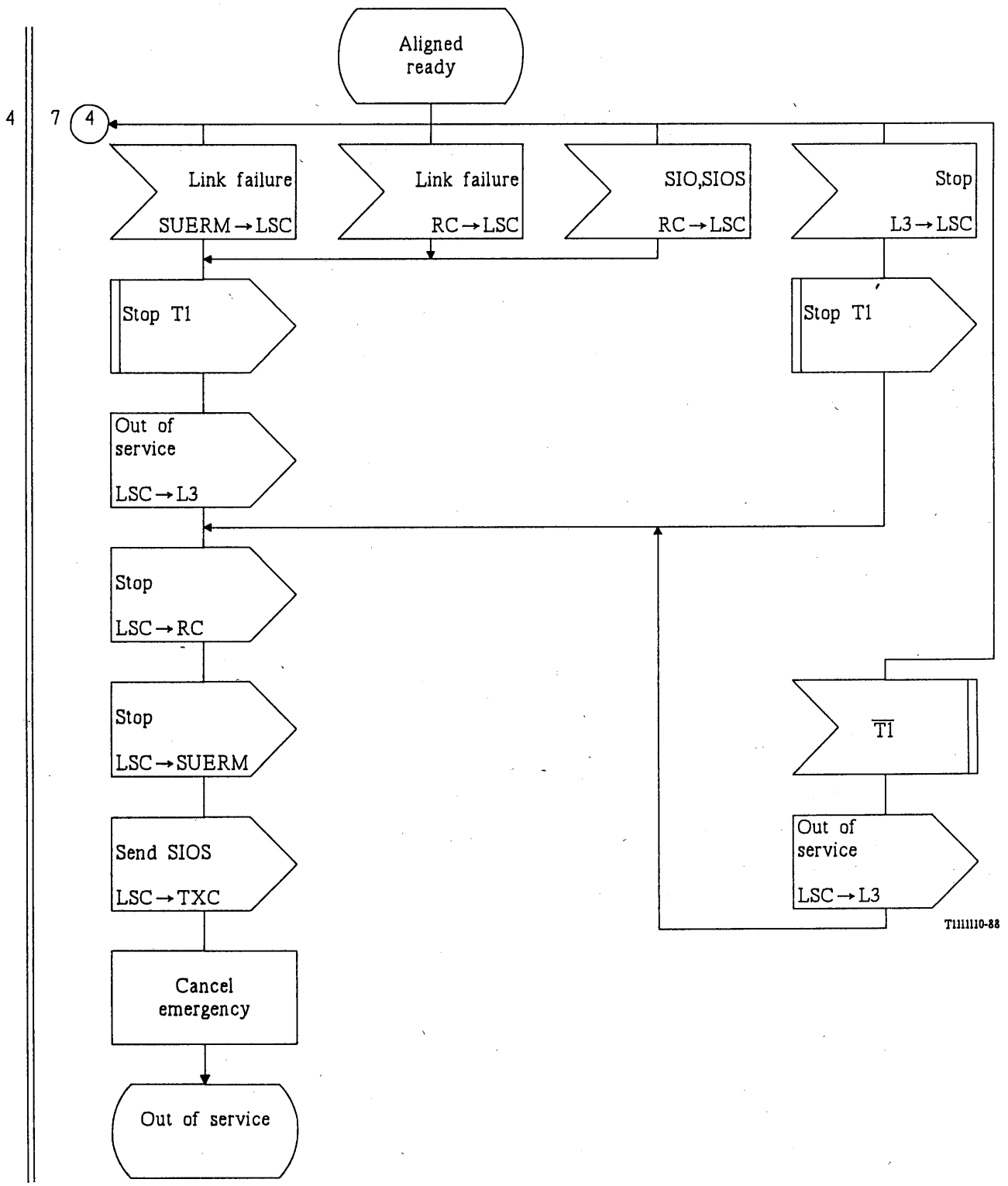
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 5 of 14)

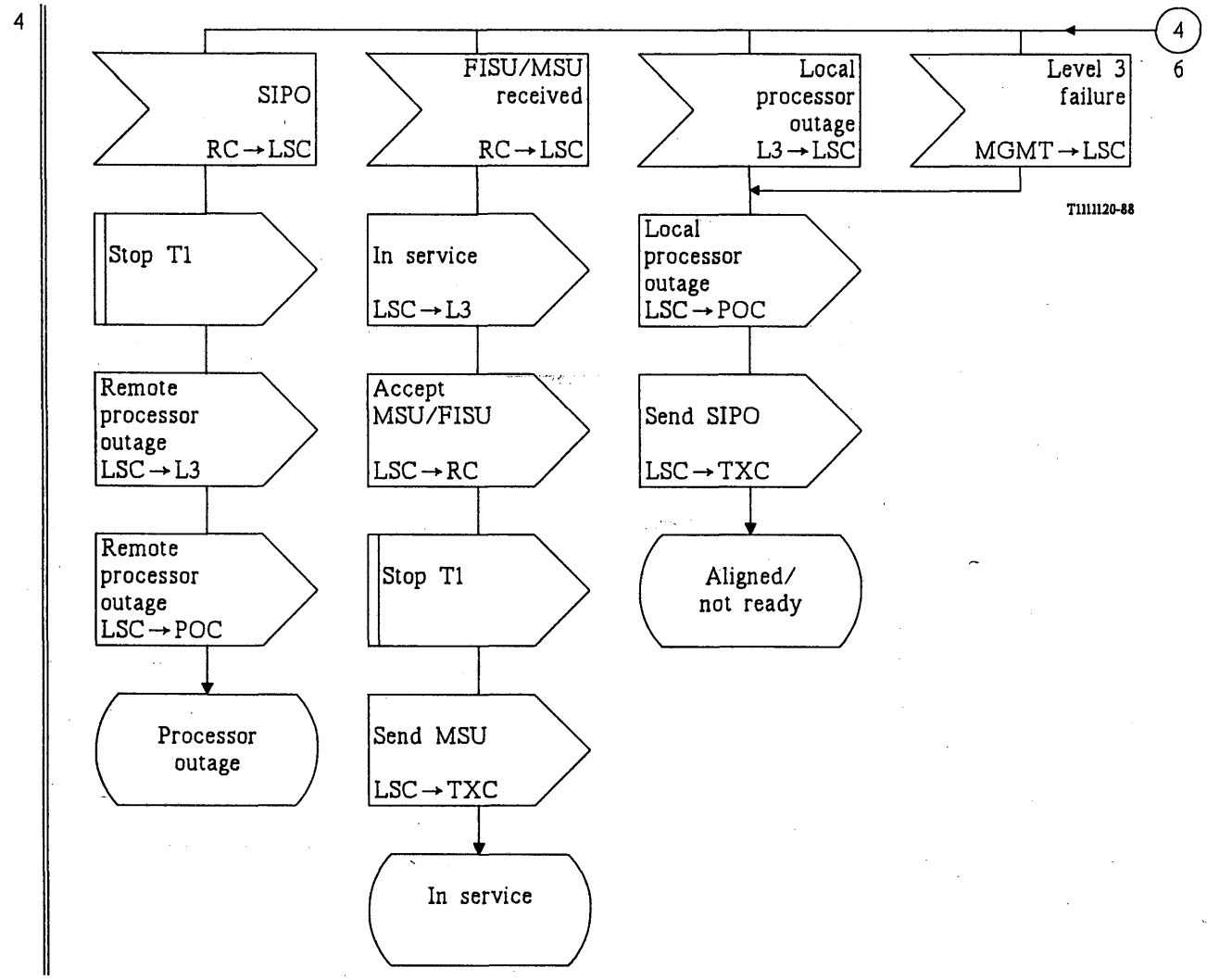
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 6 of 14)

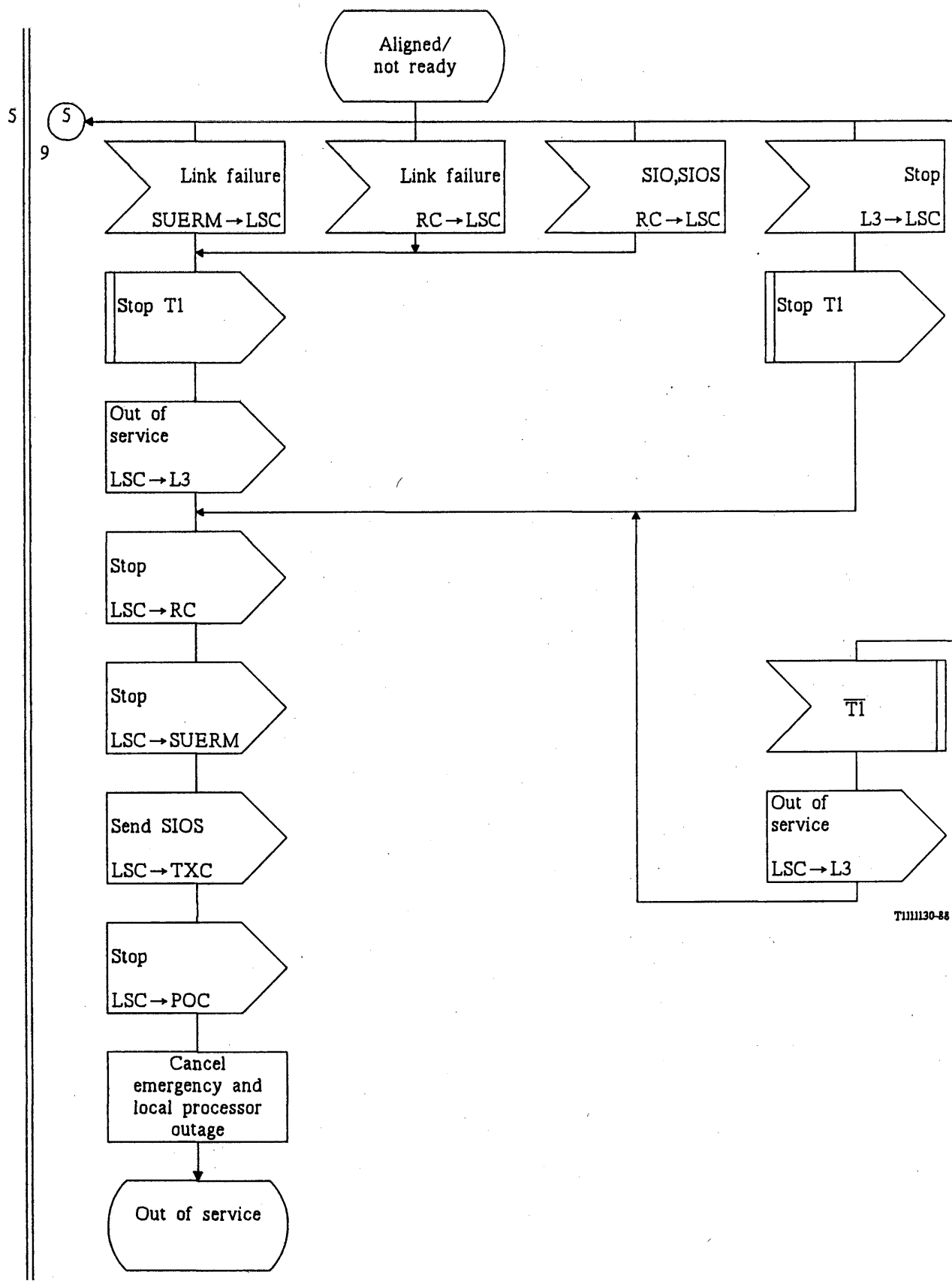
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 7 of 14)

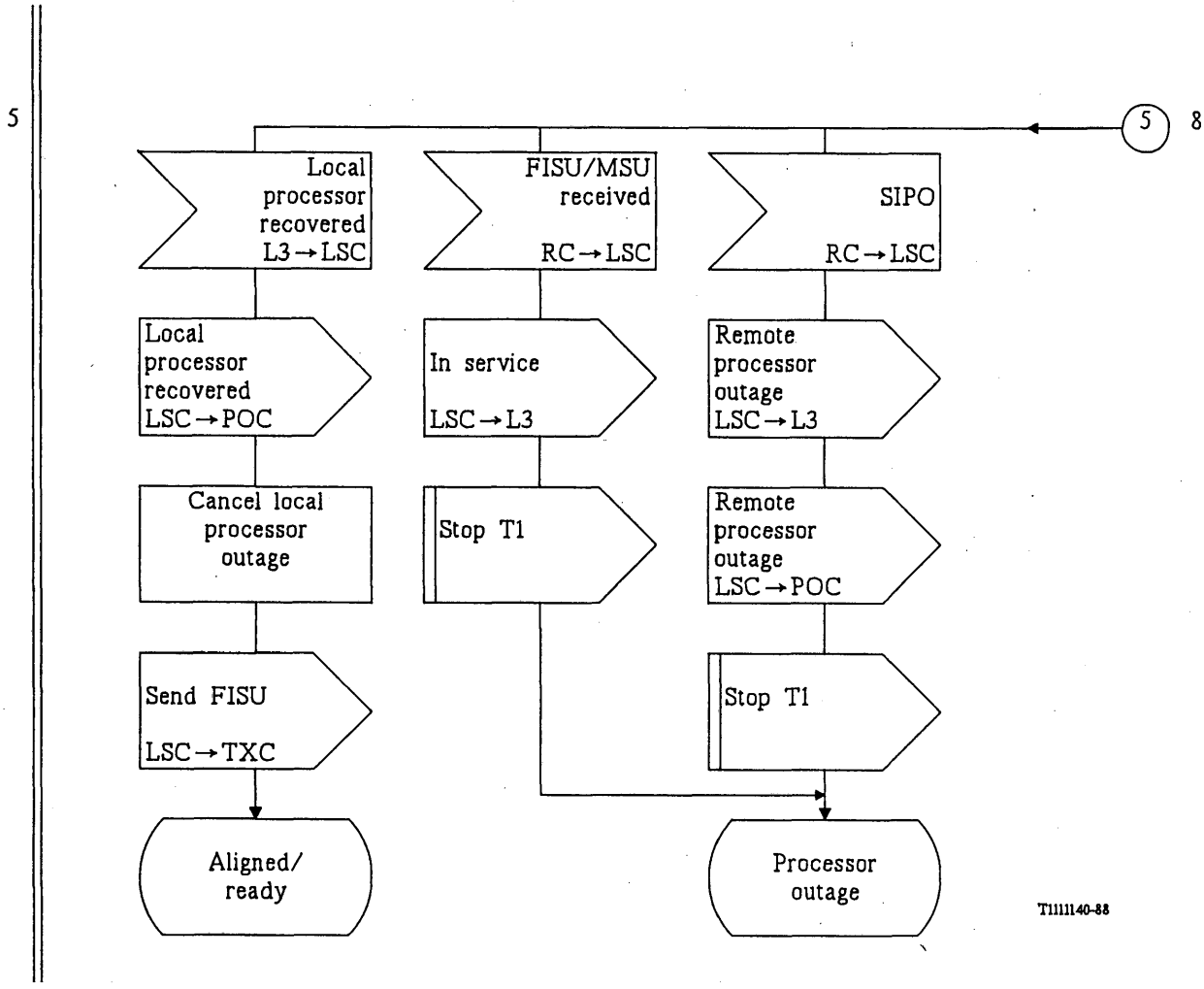
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 8 of 14)

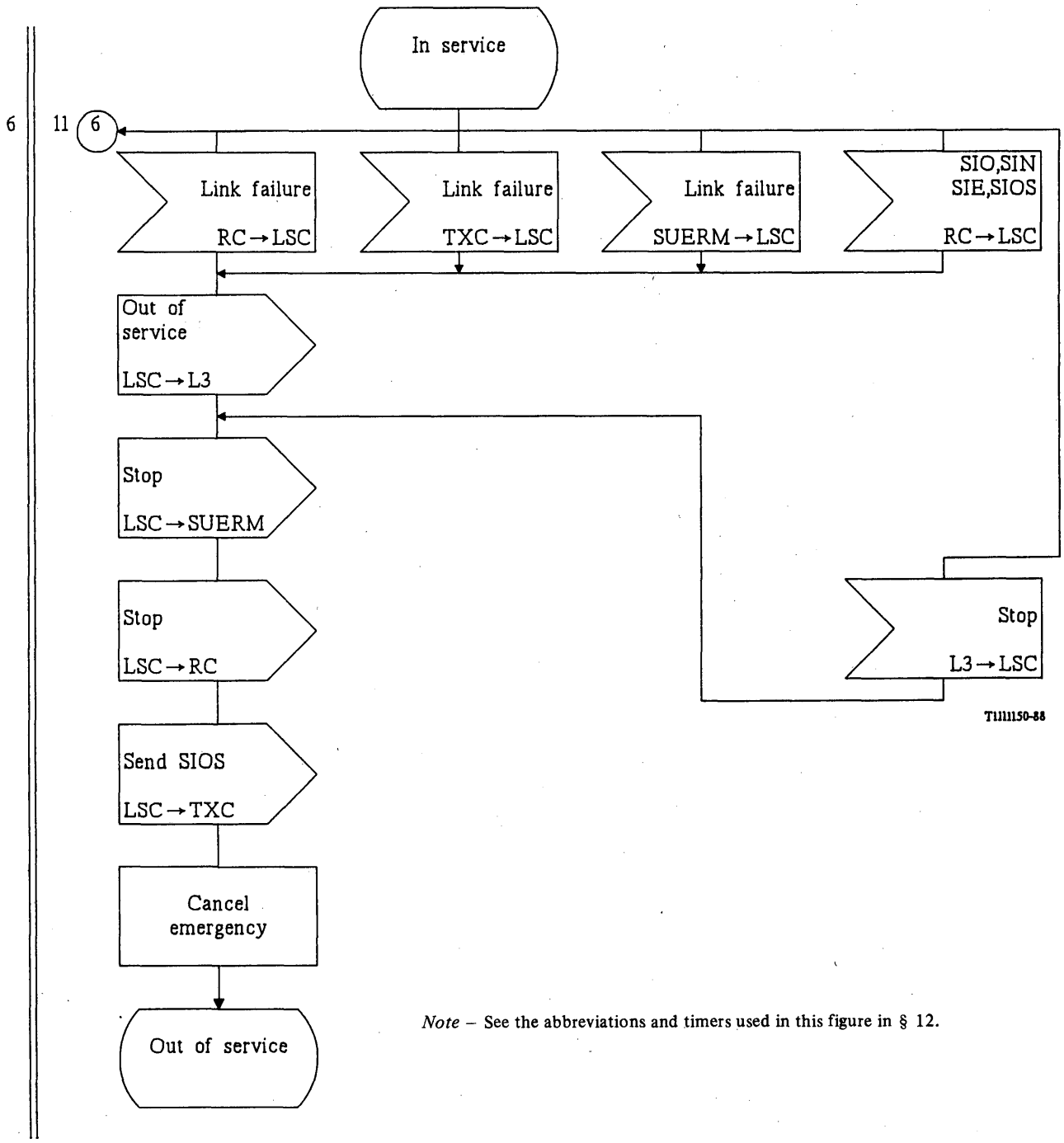
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 9 of 14)

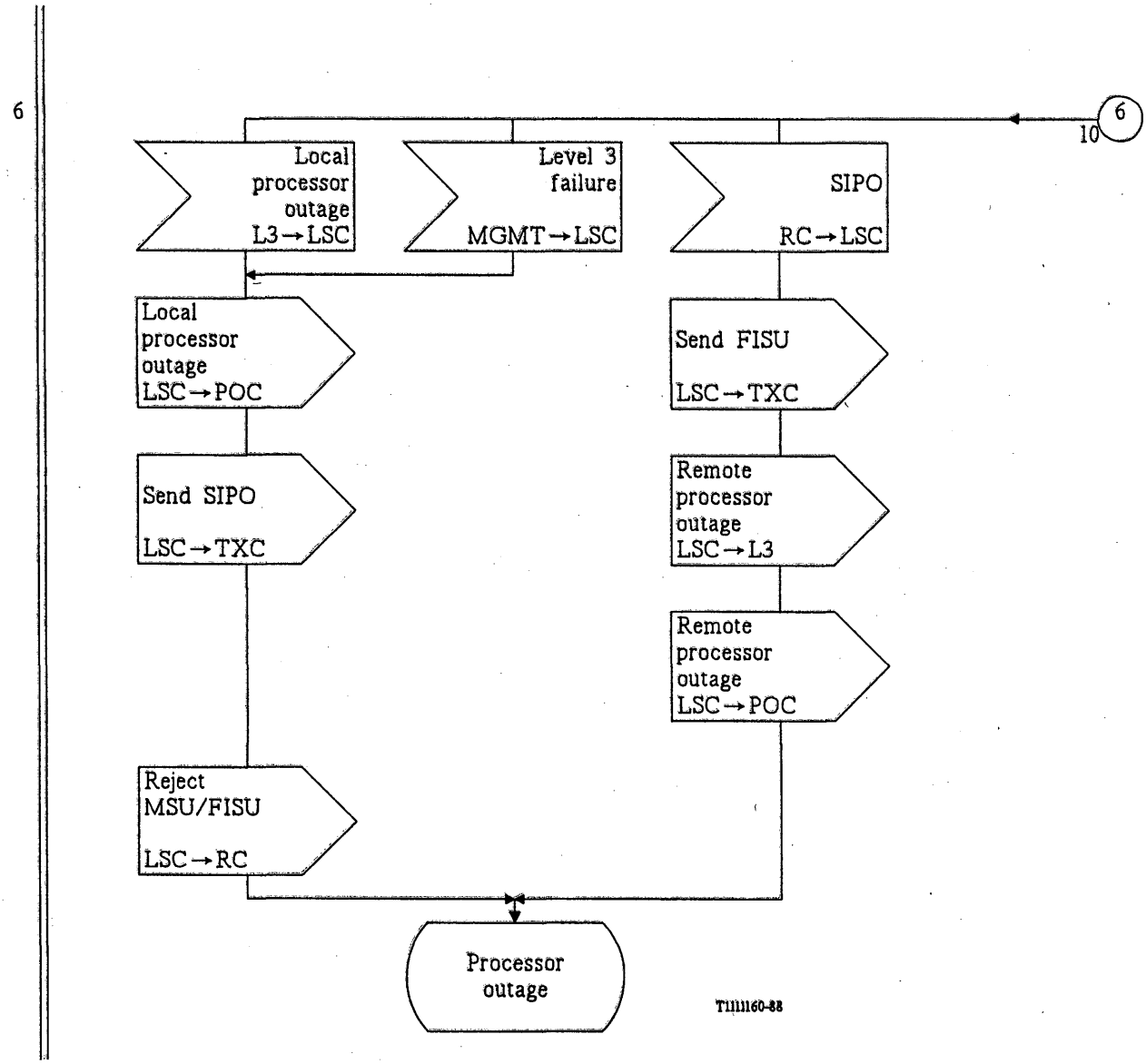
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 10 of 14)

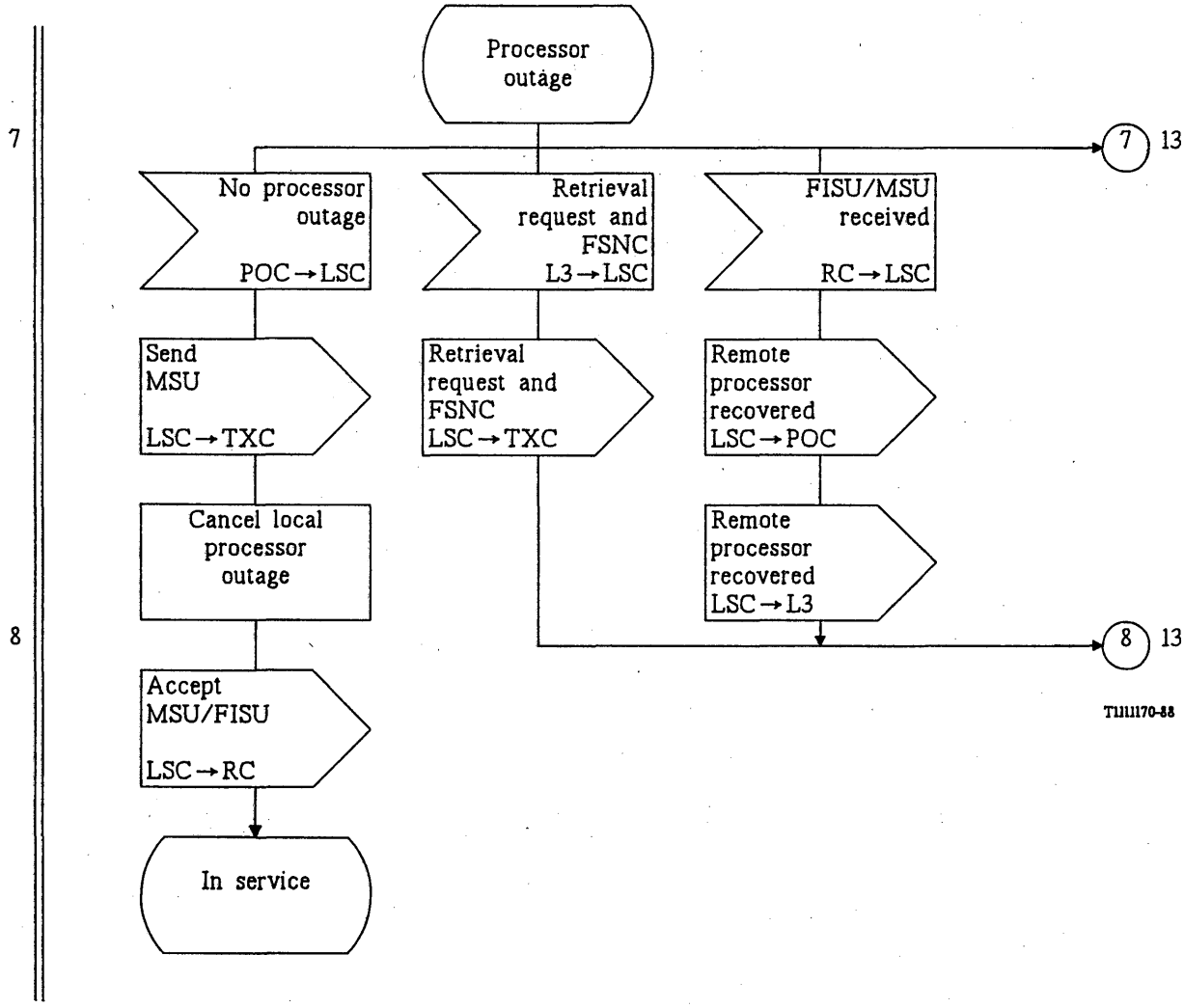
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 11 of 14)

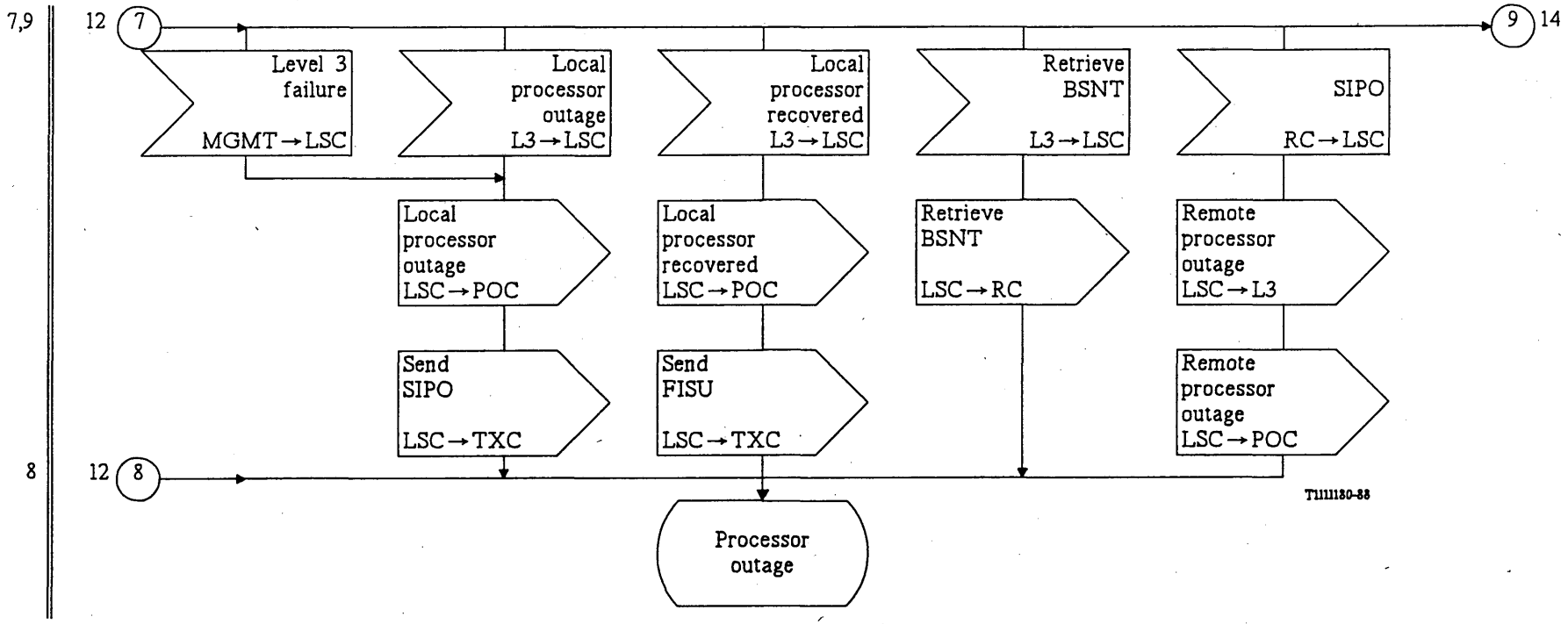
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 12 of 14)

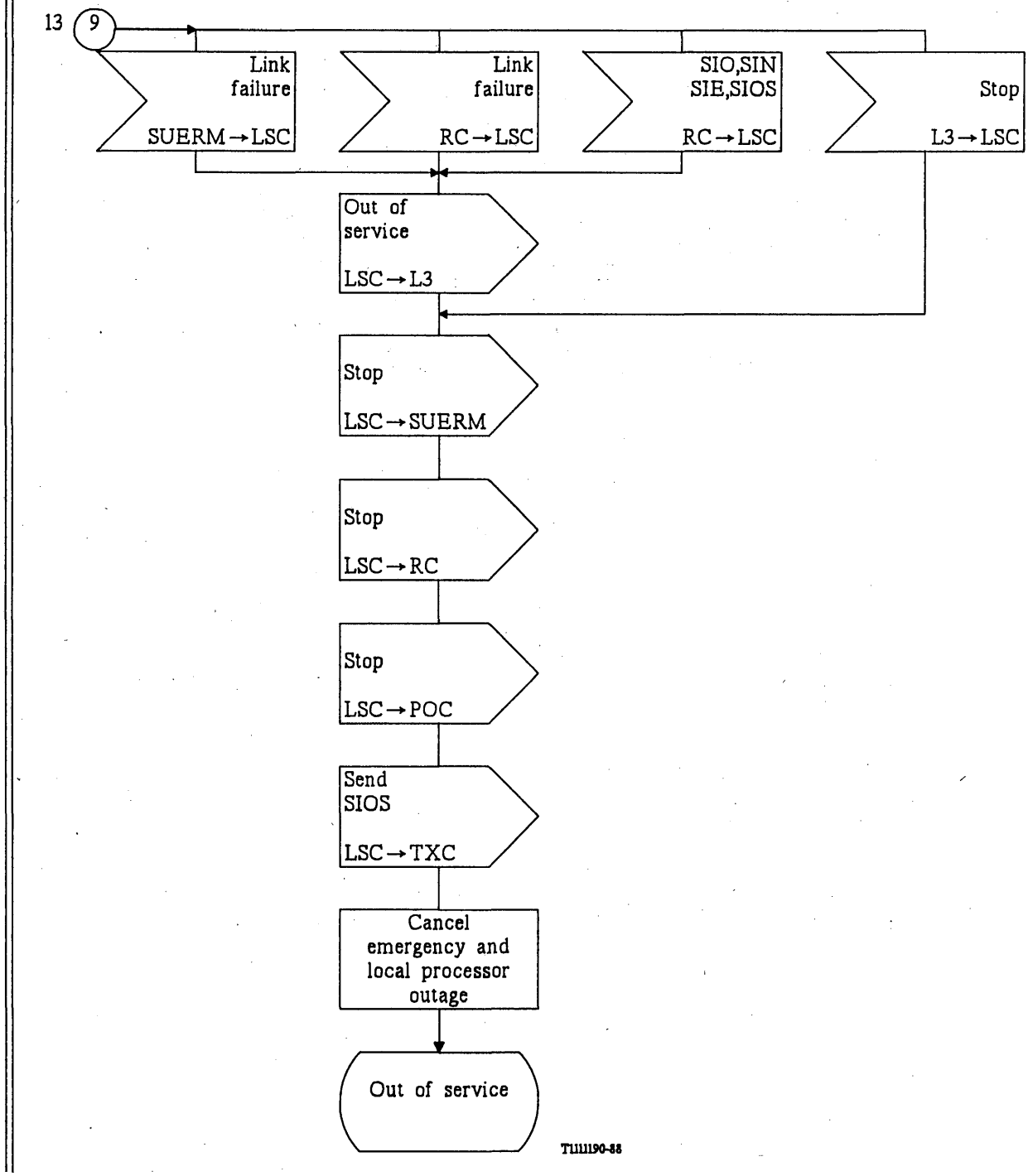
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 13 of 14)

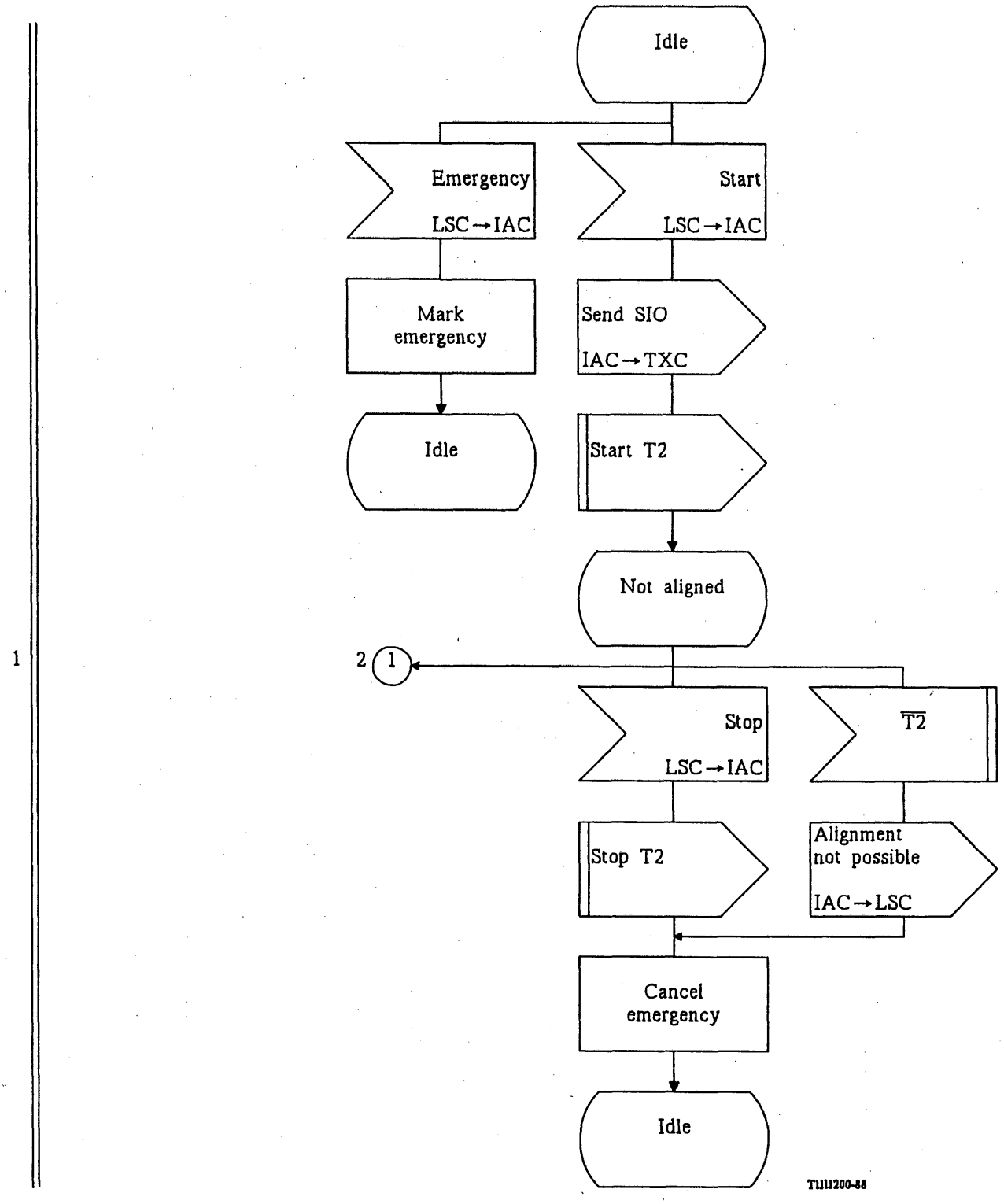
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 8/Q.703 (sheet 14 of 14)

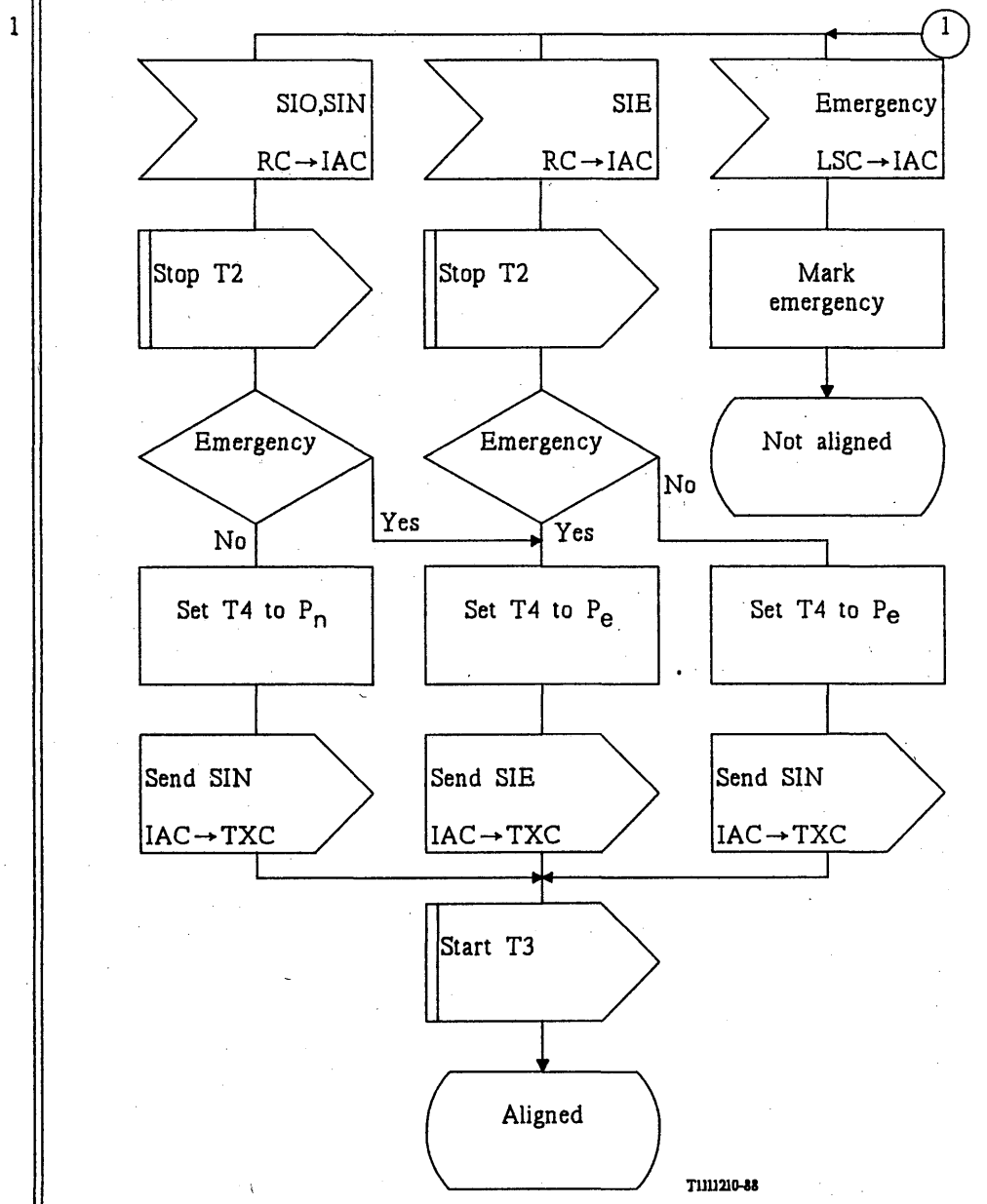
**Link state control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 9/Q.703 (sheet 1 of 6)

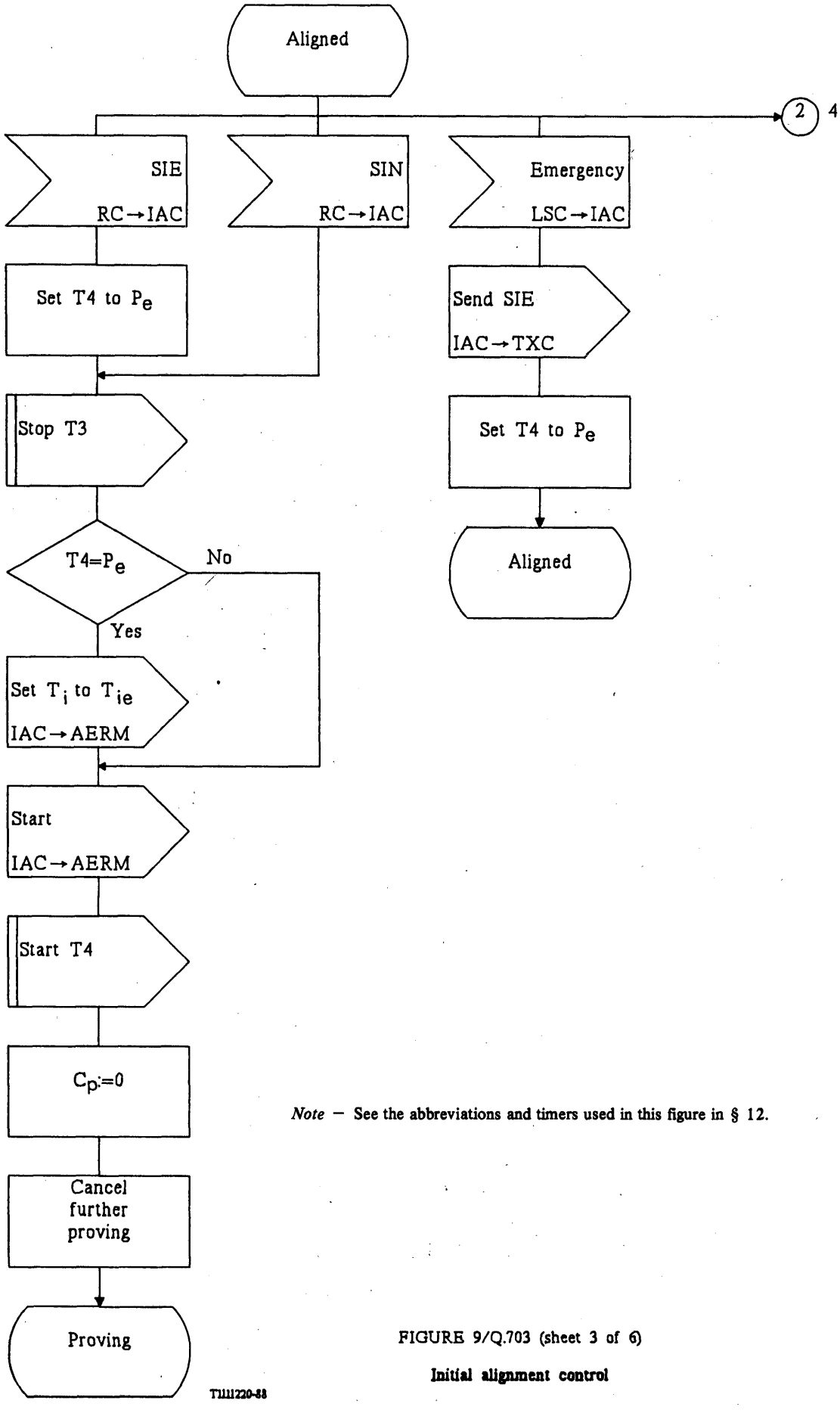
**Initial alignment control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 9/Q.703 (sheet 2 of 6)

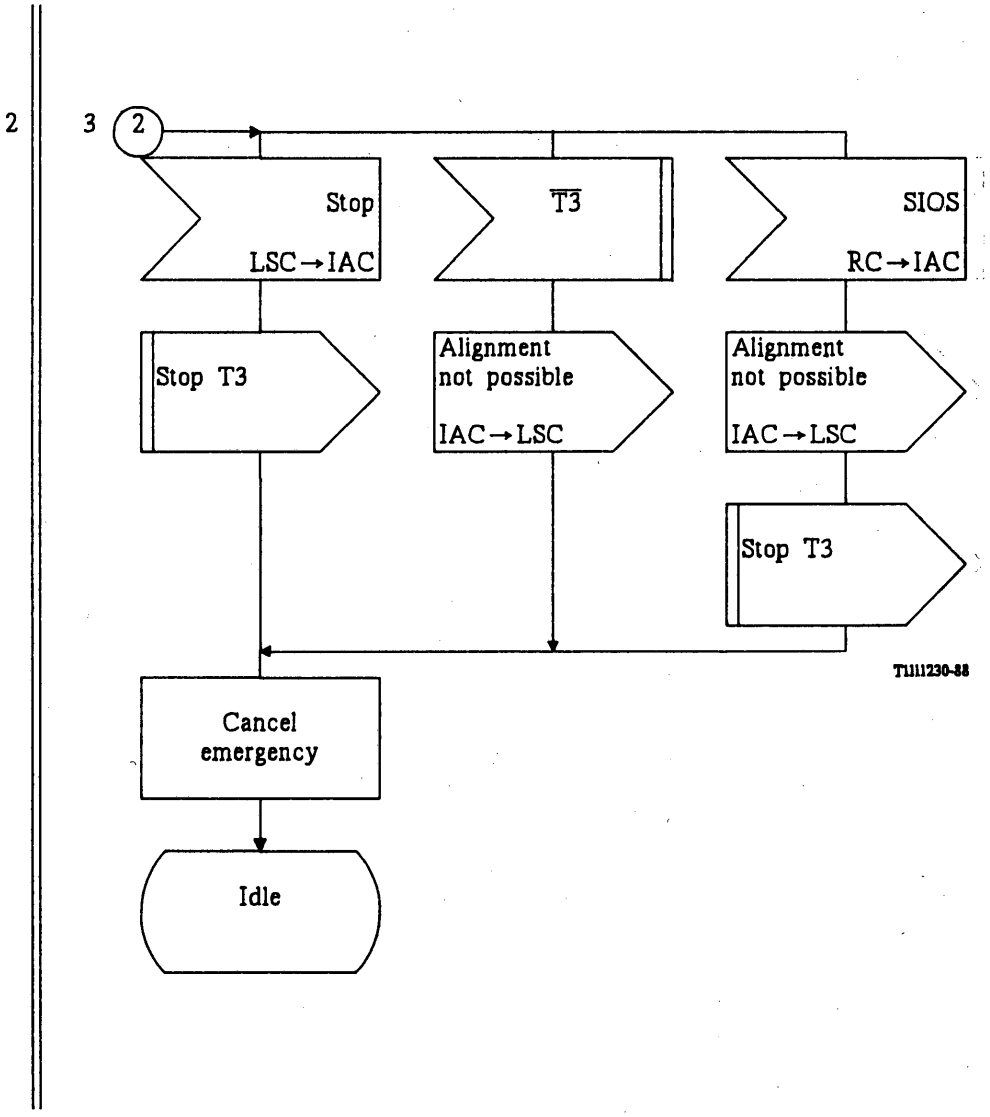
**Initial alignment control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 9/Q.703 (sheet 3 of 6)

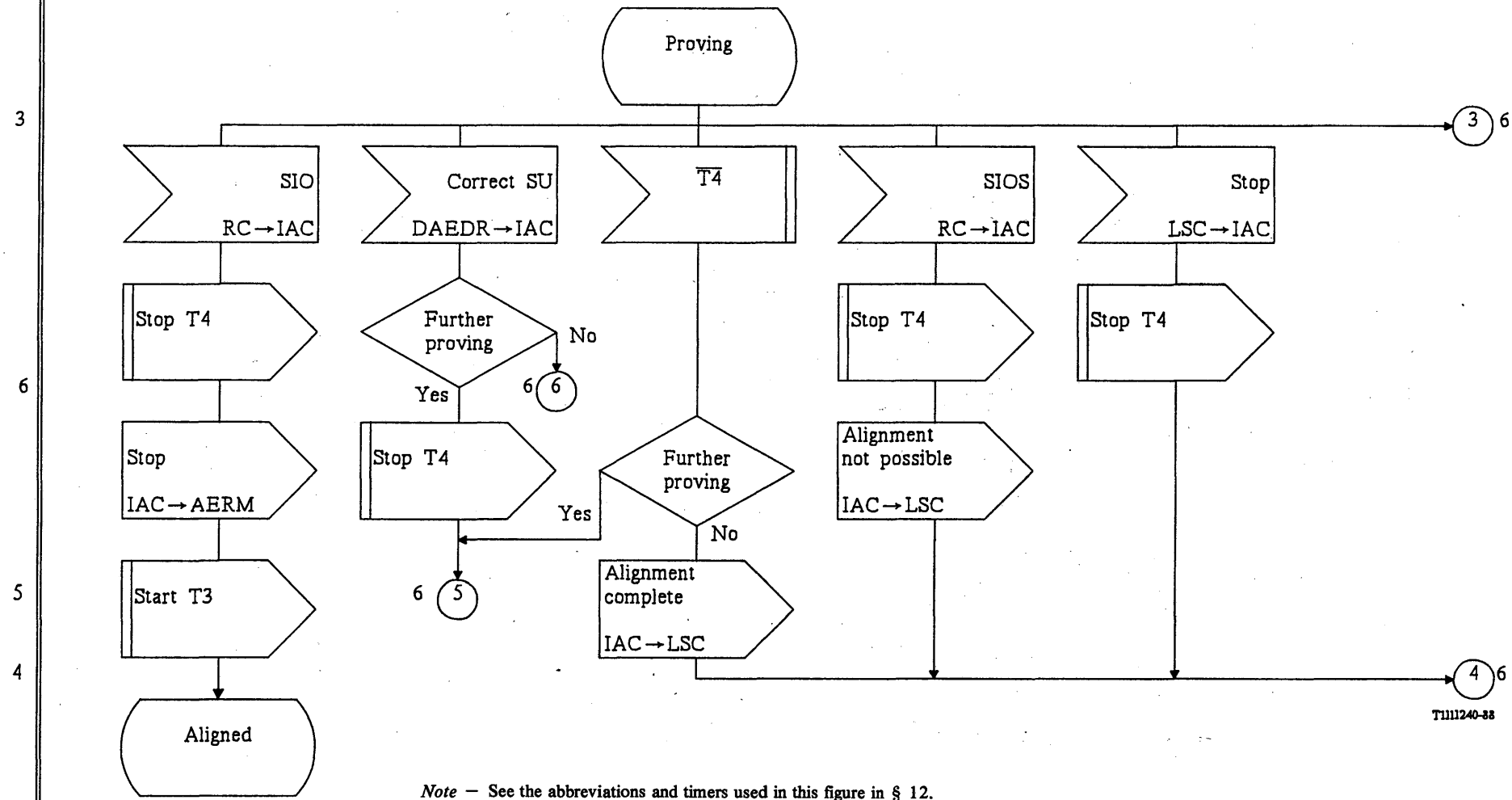
**Initial alignment control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 9/Q.703 (sheet 4 of 6)

**Initial alignment control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 9/Q.703 (sheet 5 of 6)

**Initial alignment control**

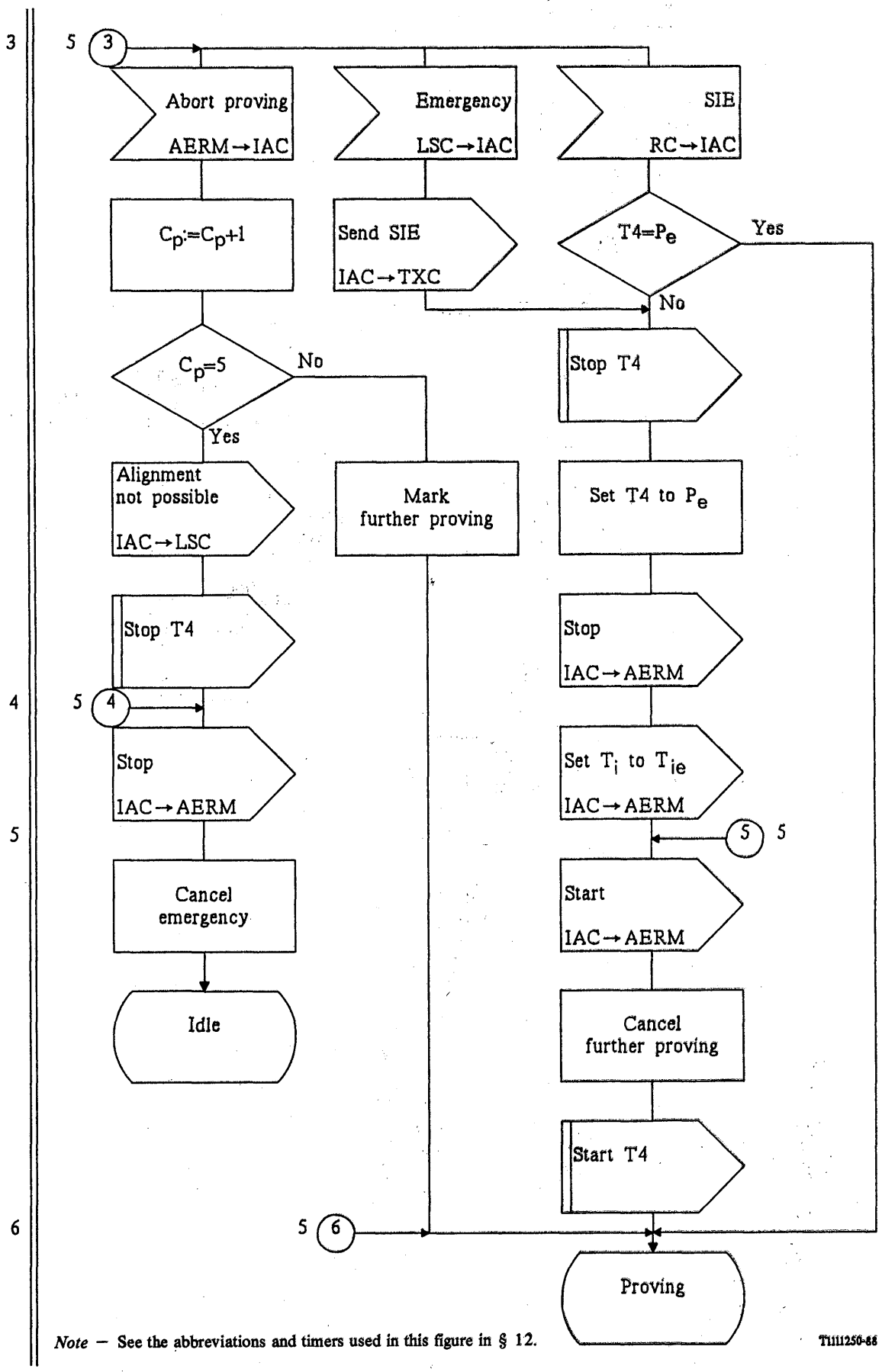
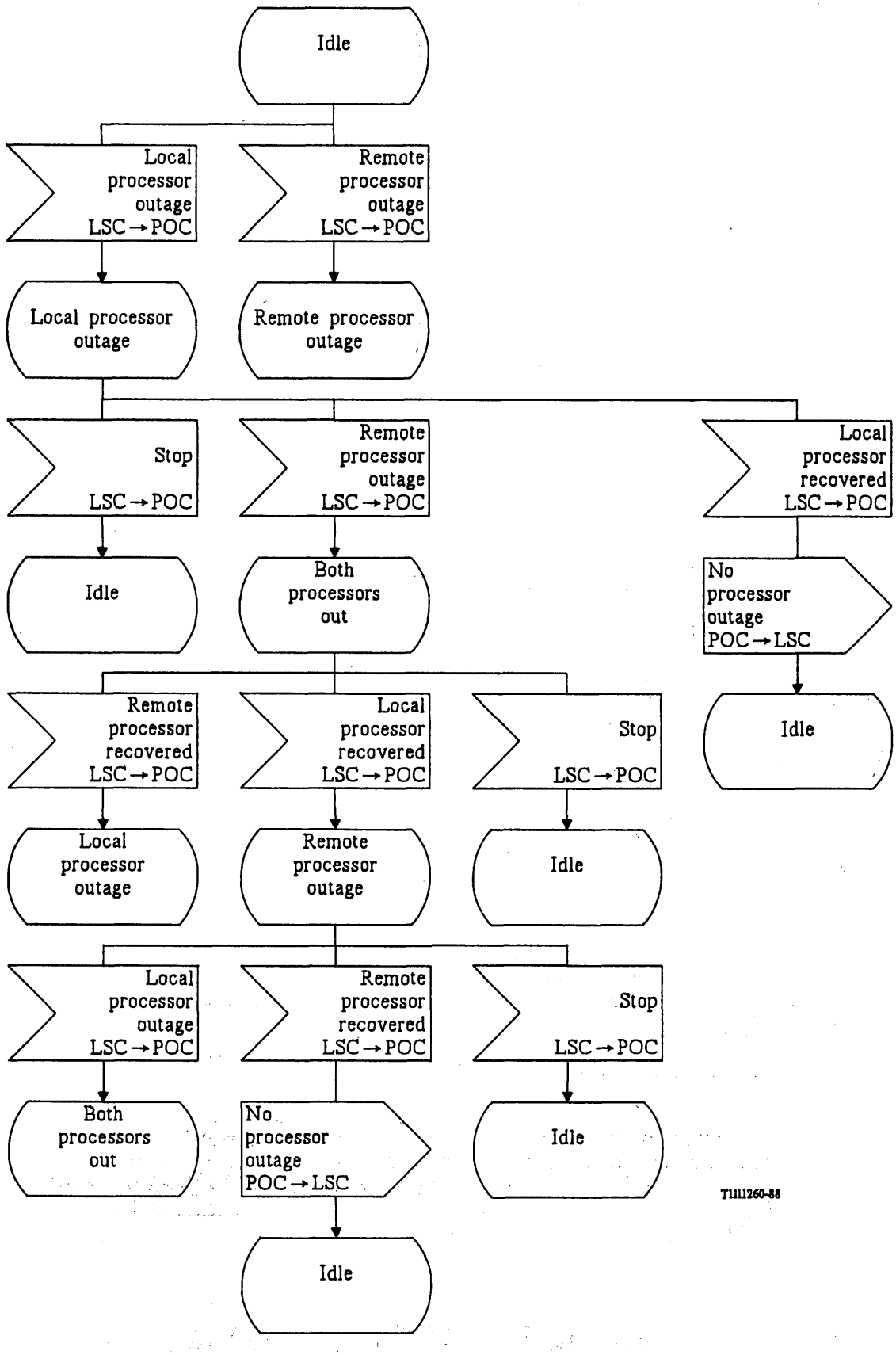



FIGURE 9/Q.703 (sheet 6 of 6)

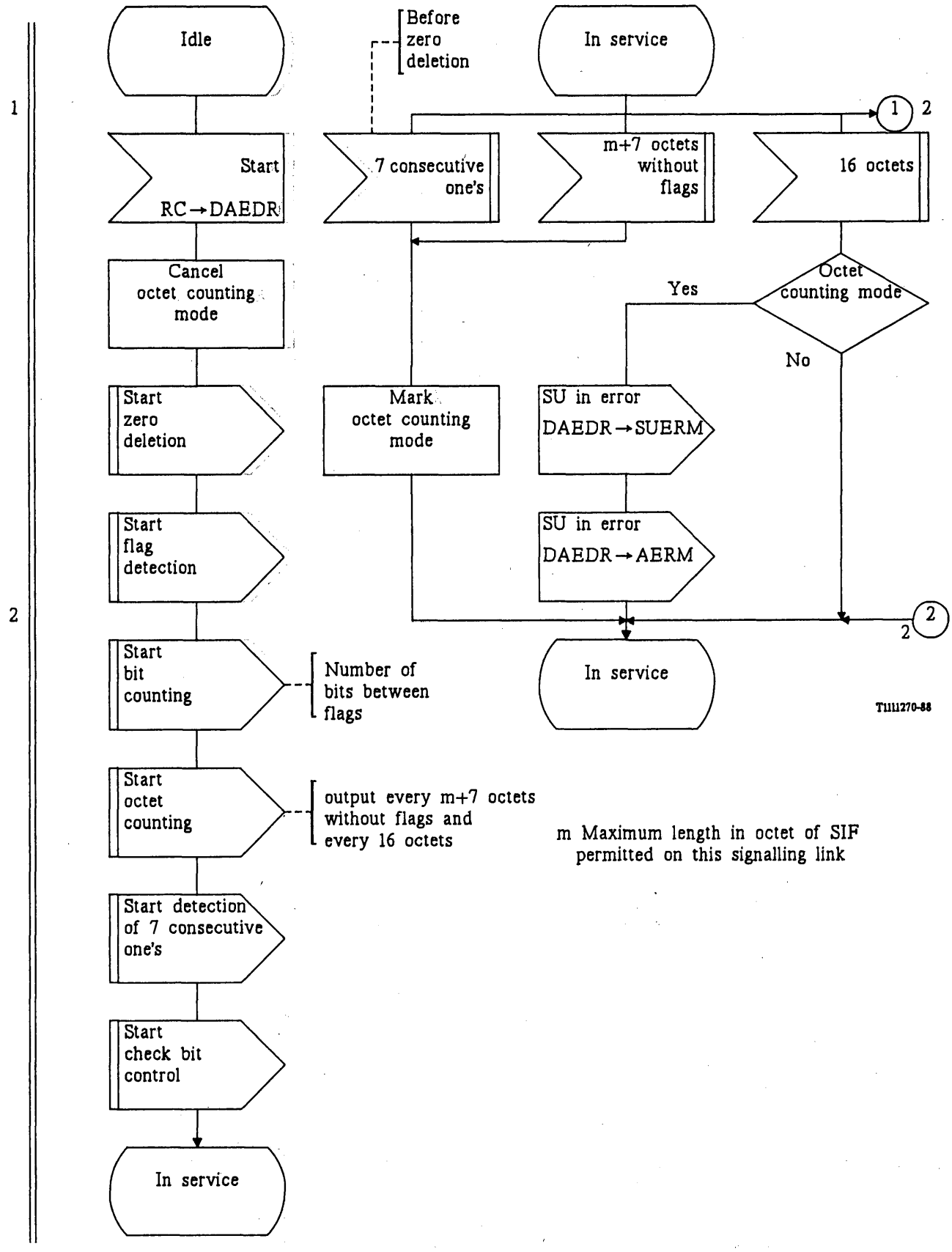
**Initial alignment control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 10/Q.703

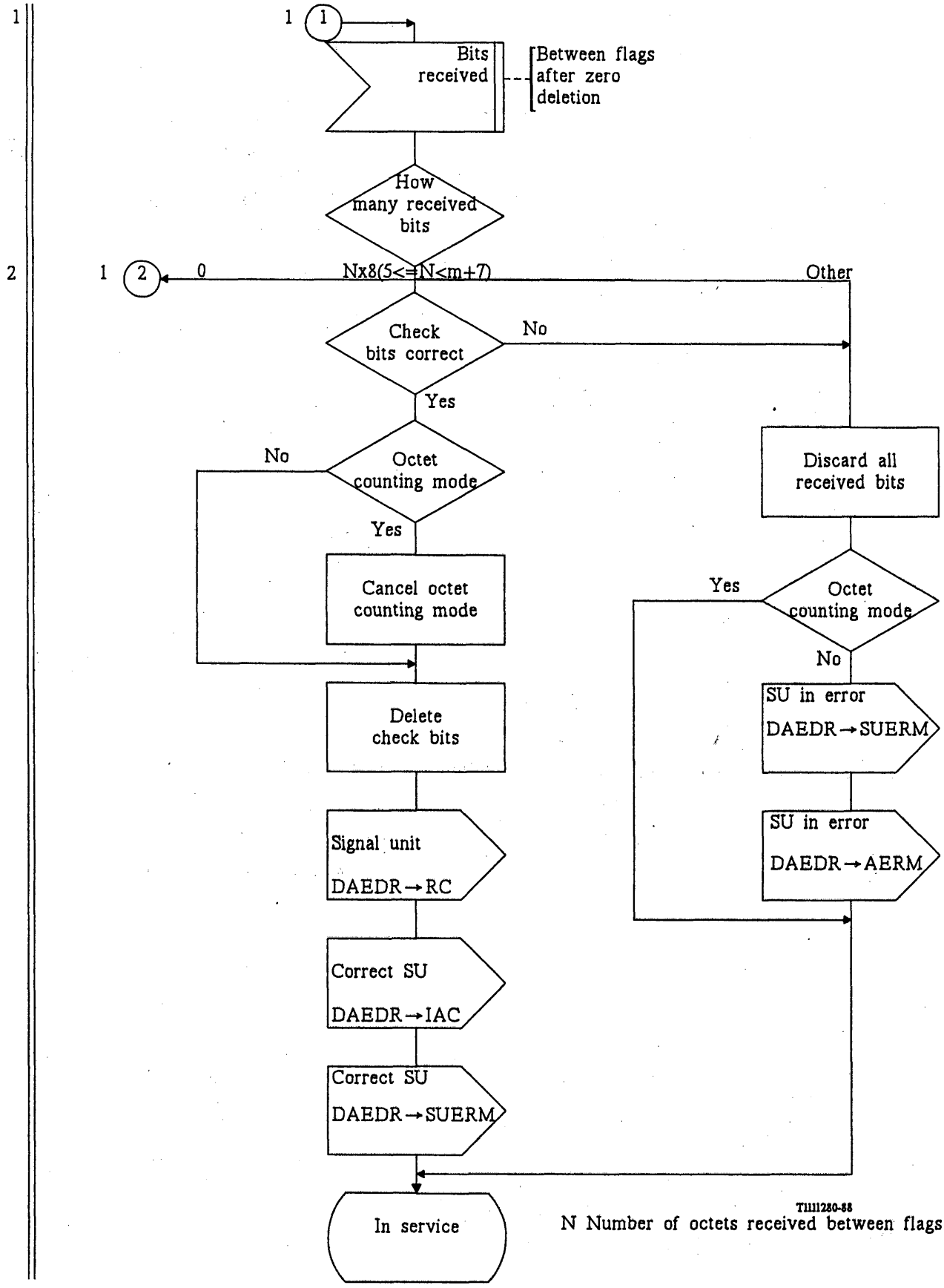
**Processor outage control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 11/Q.703 (sheet 1 of 2)

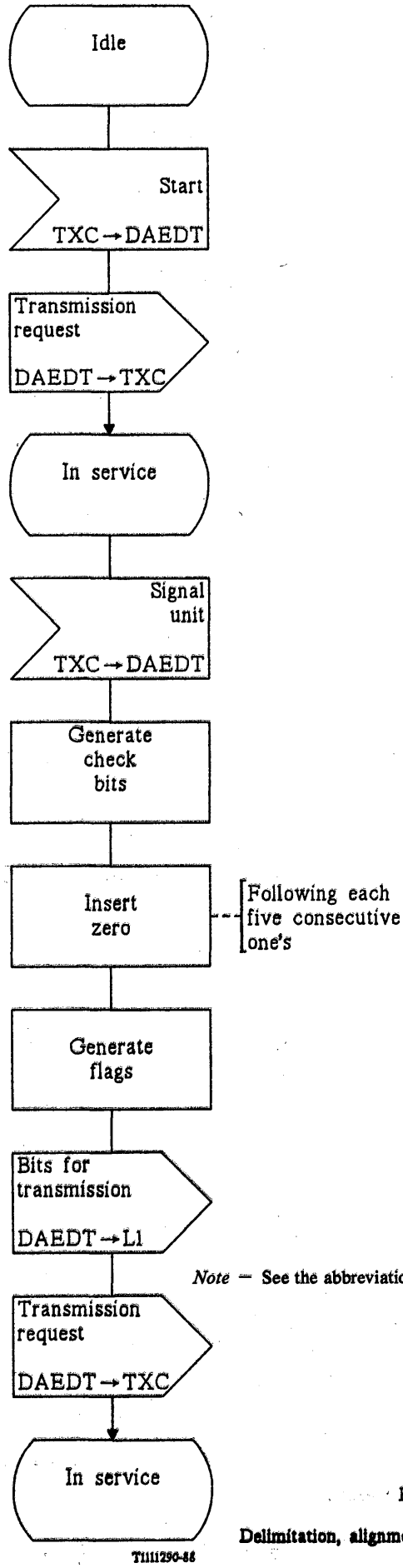
**Delimitation, alignment and error detection (receiving)**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 11/Q.703 (sheet 2 of 2)

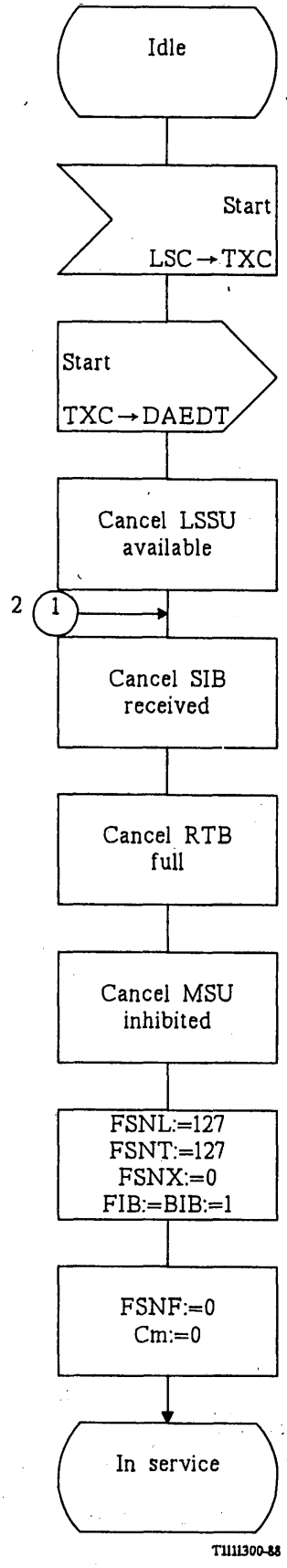
**Delimitation, alignment and error detection (receiving)**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 12/Q.703

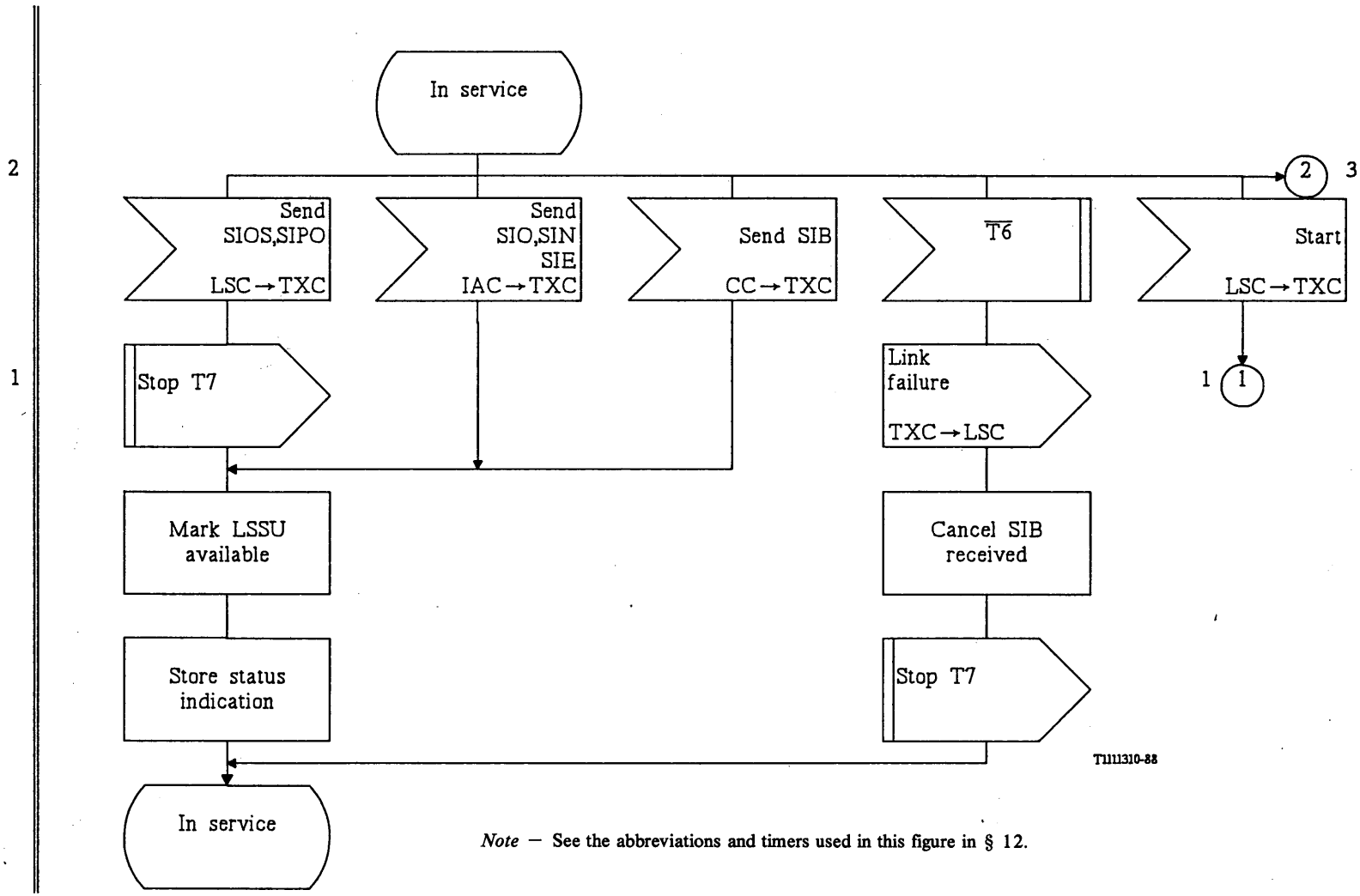
**Delimitation, alignment and error detection (transmitting)**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 13/Q.703 (sheet 1 of 6)

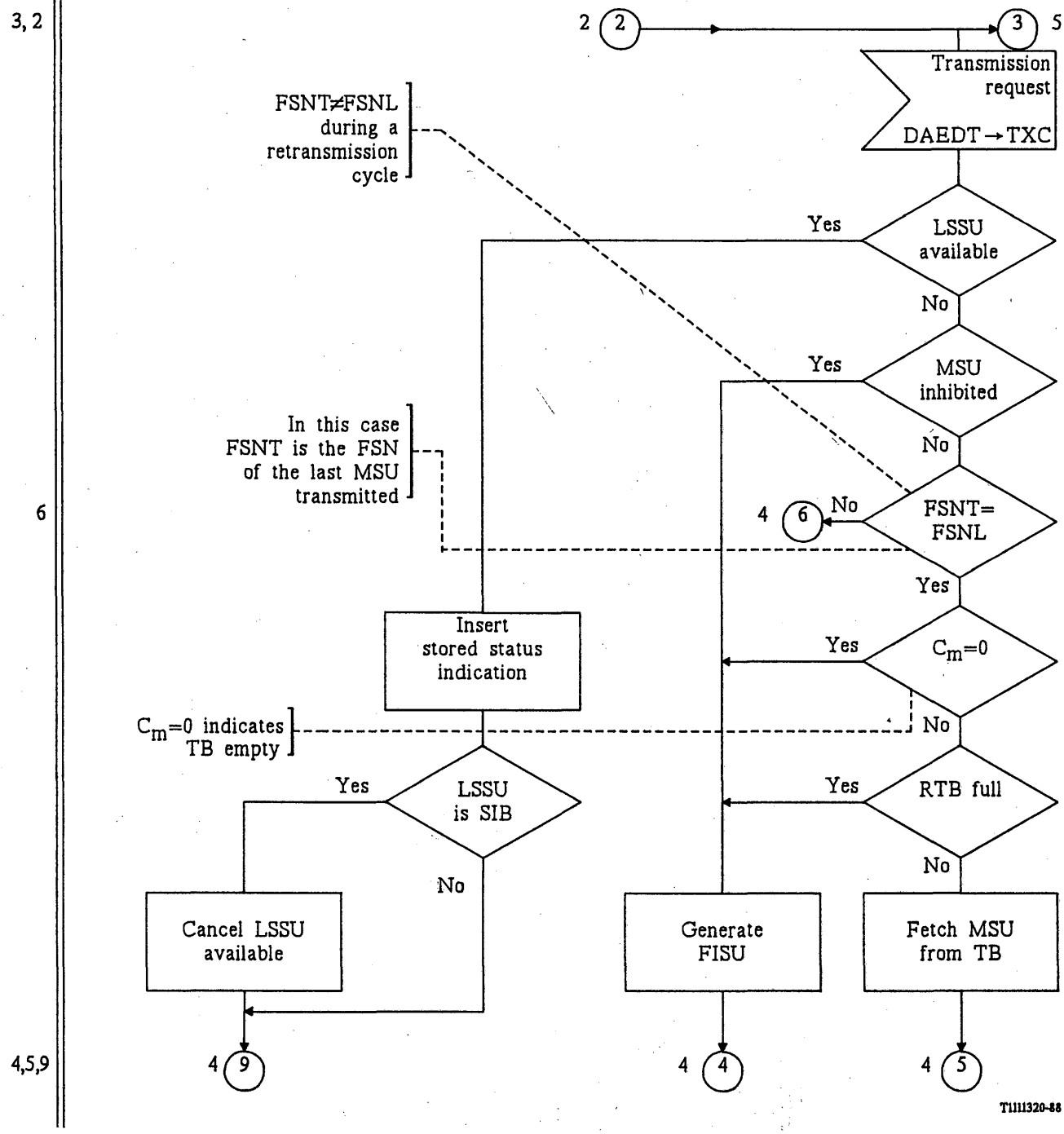
**Basic transmission control**




*Note* — See the abbreviations and timers used in this figure in § 12.

FIGURE 13/Q.703 (sheet 2 of 6)

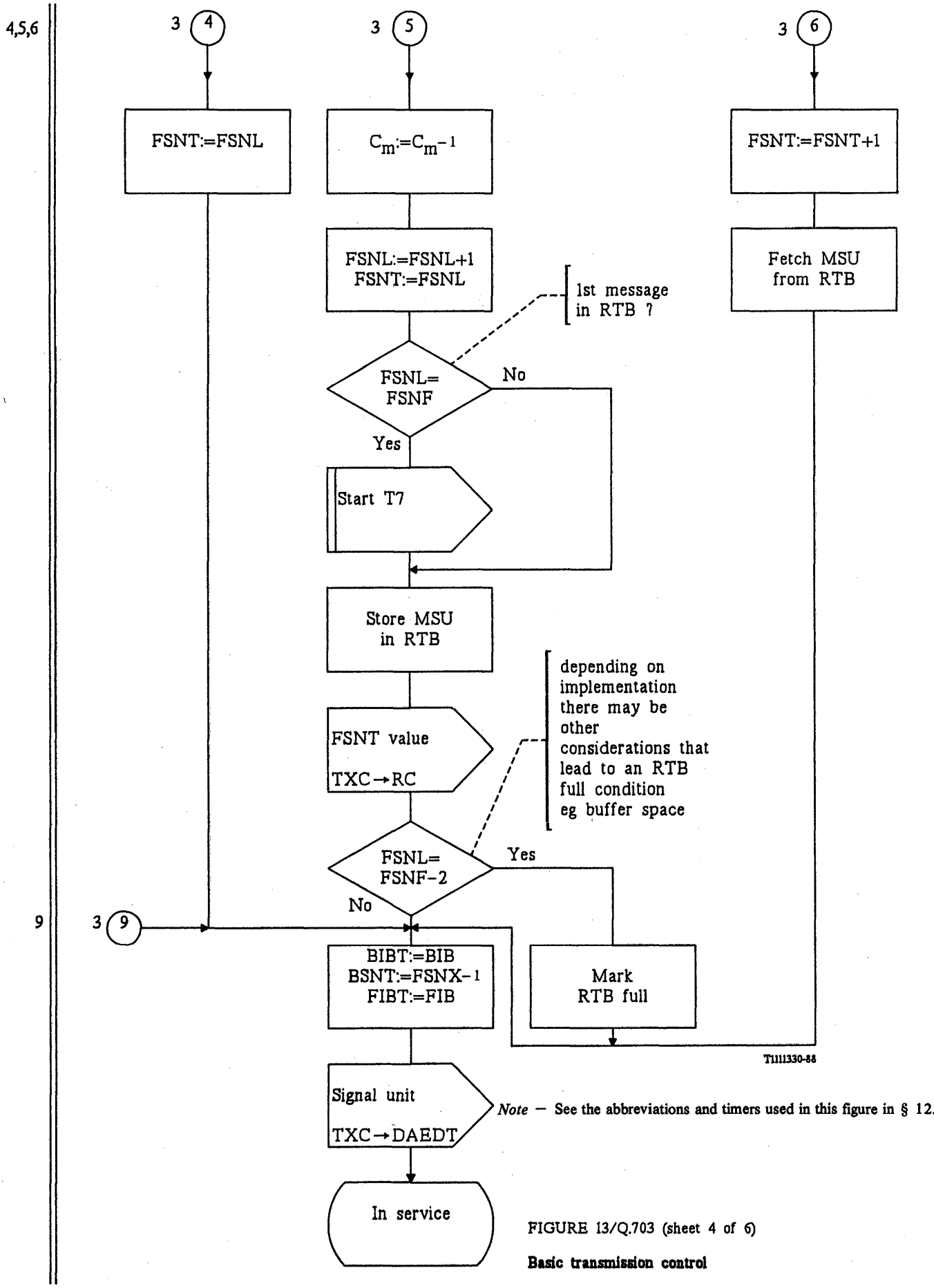
**Basic transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 13/Q.703 (sheet 3 of 6)

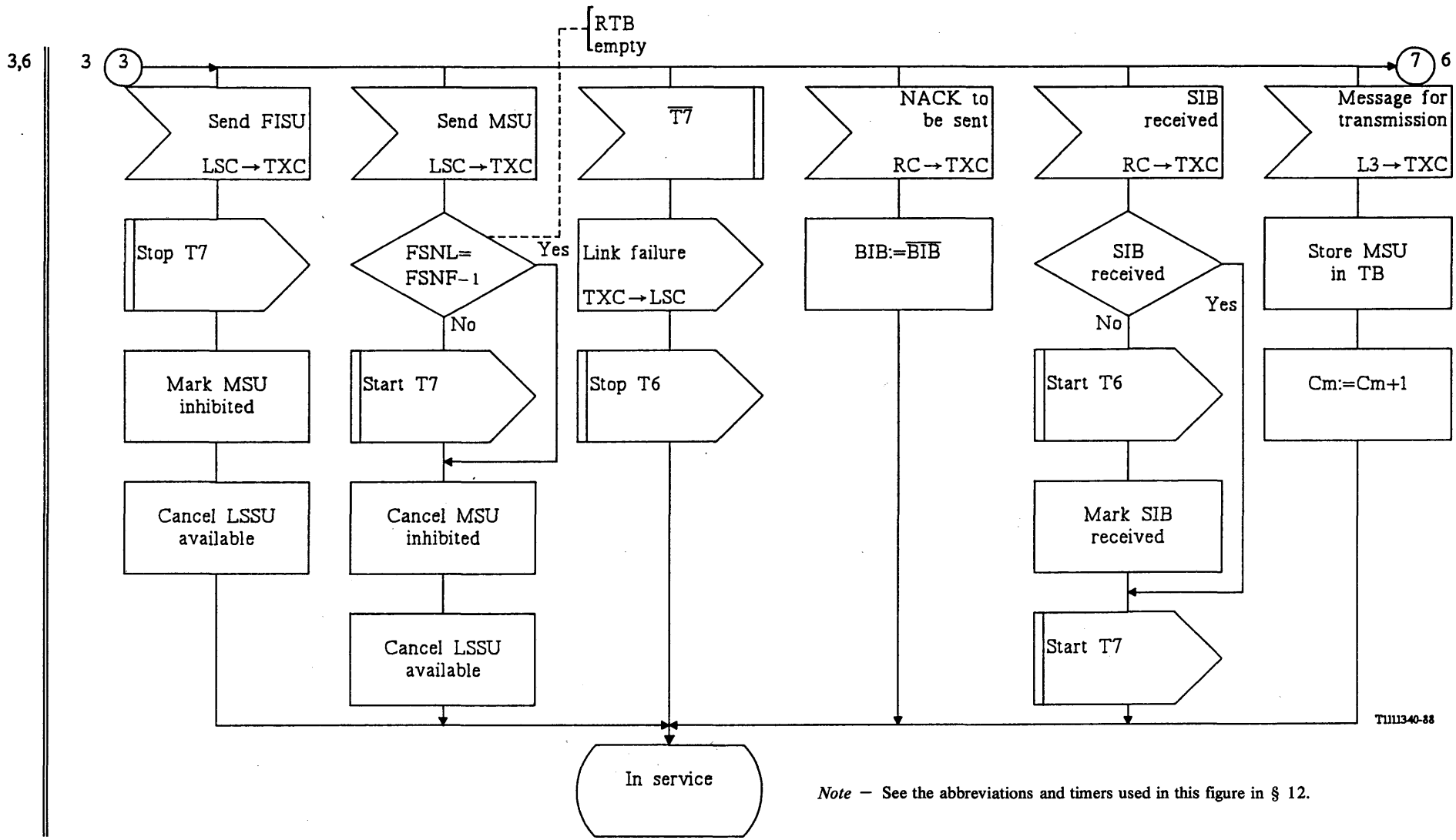
**Basic transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 13/Q.703 (sheet 4 of 6)

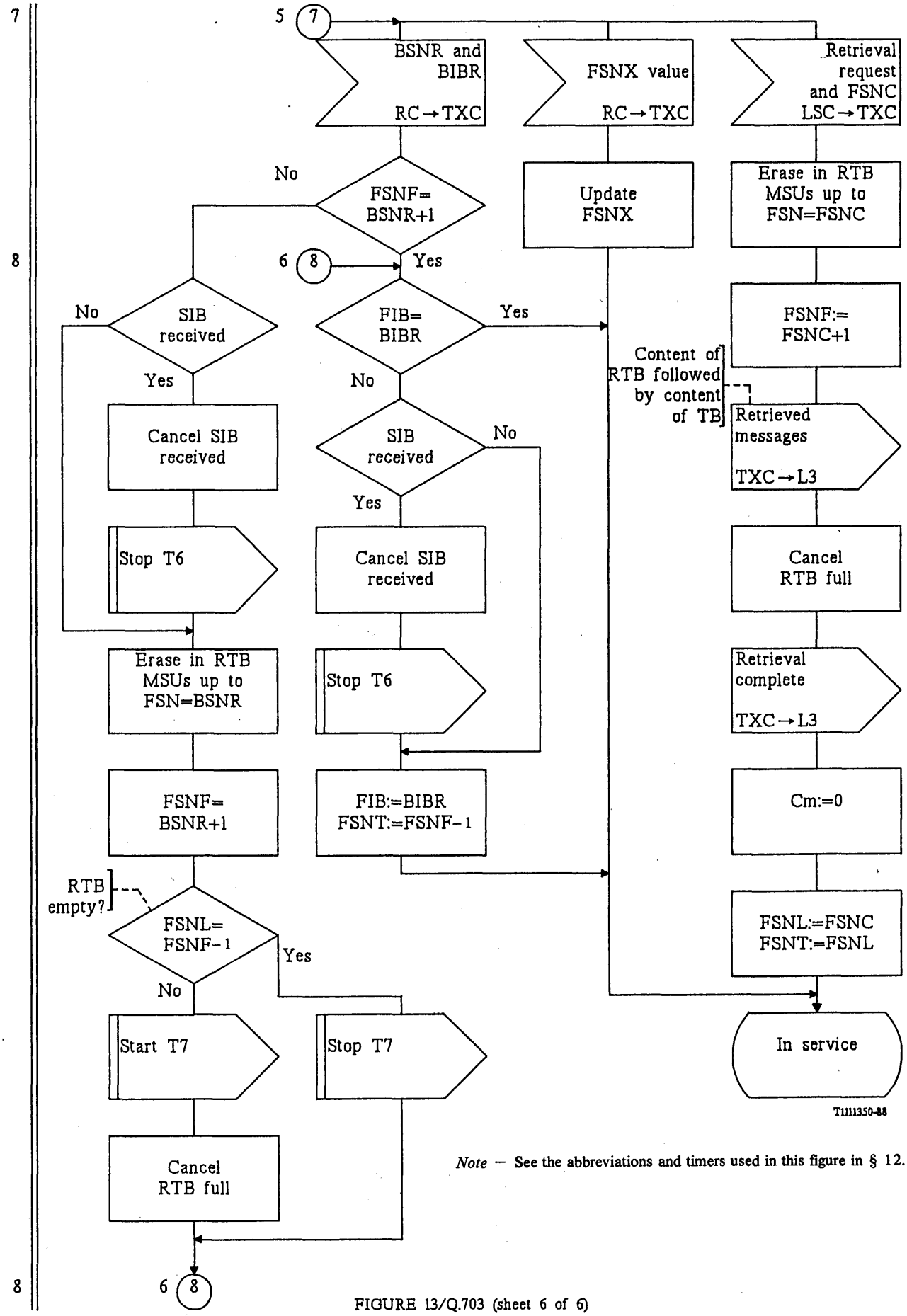
**Basic transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 13/Q.703 (sheet 5 of 6)

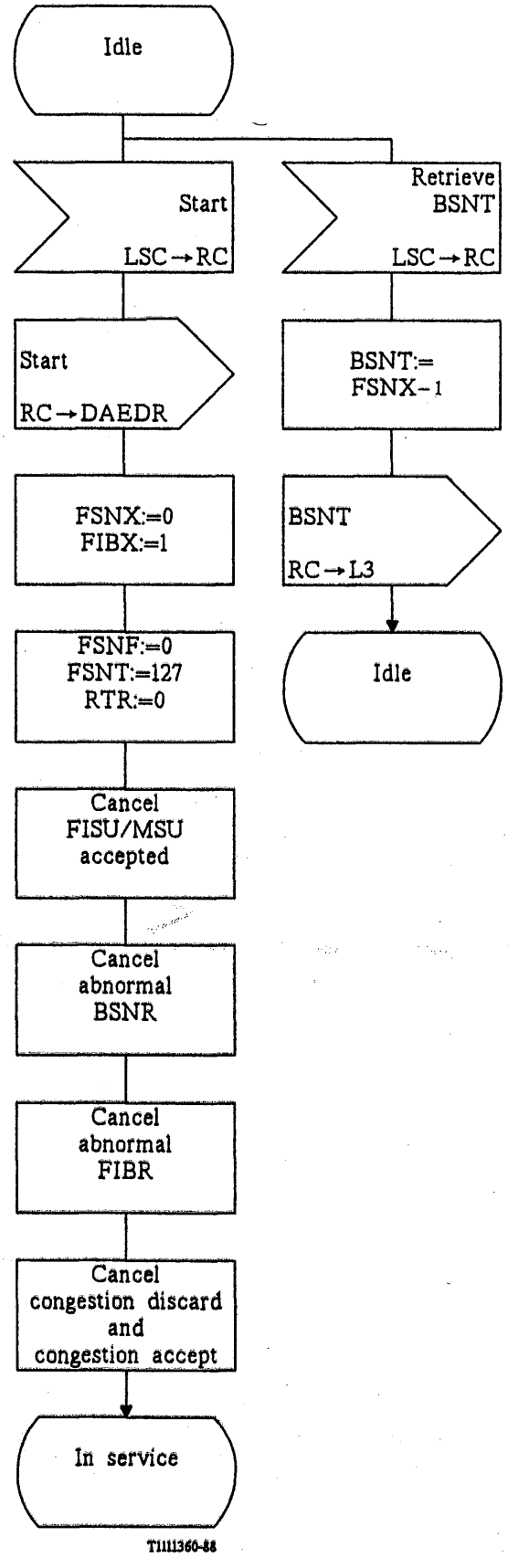
**Basic transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 13/Q.703 (sheet 6 of 6)

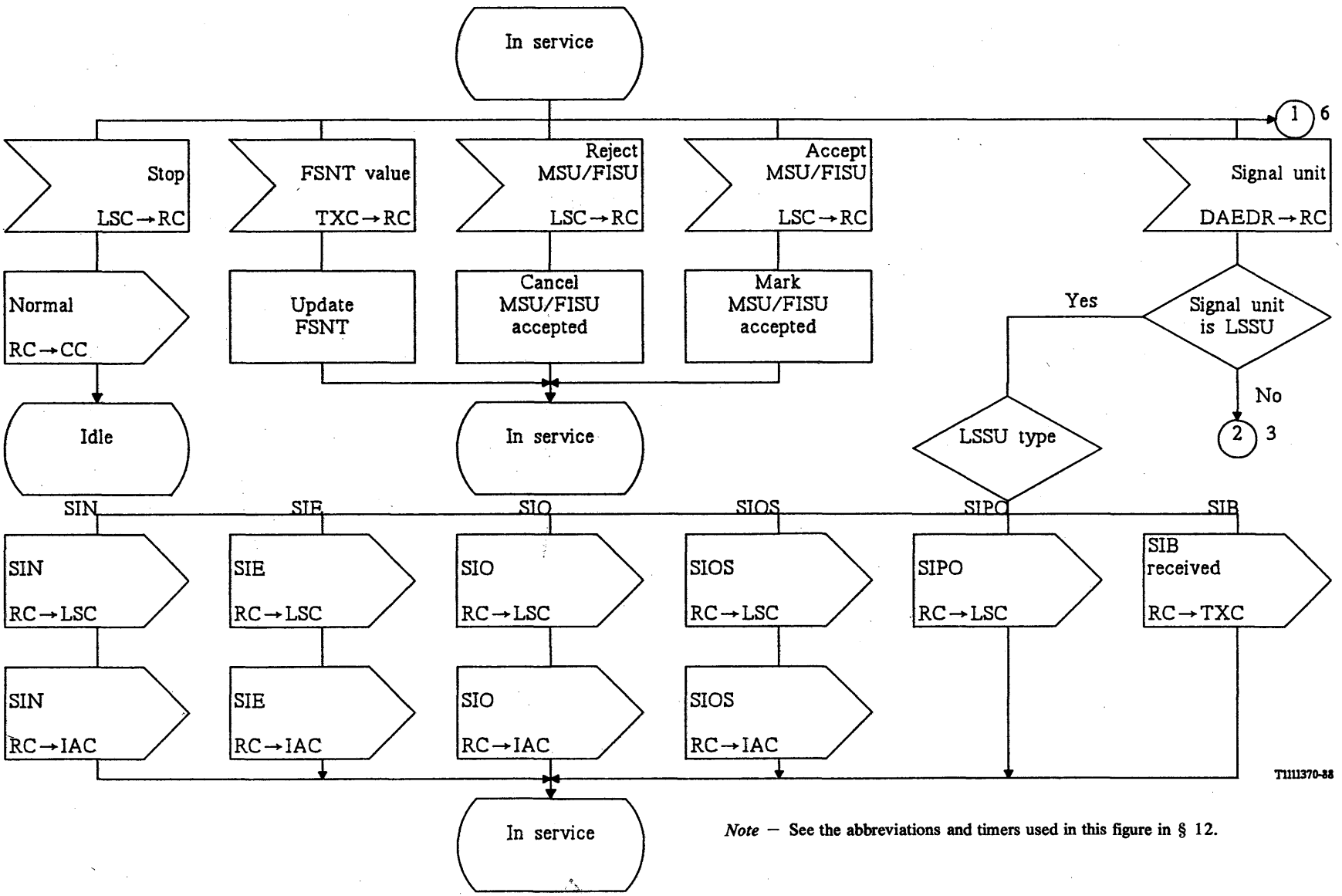
**Basic transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 14/Q.703 (sheet 1 of 6)

**Basic reception control**




*Note* — See the abbreviations and timers used in this figure in § 12.

FIGURE 14/Q.703 (sheet 2 of 6)

**Basic reception control**

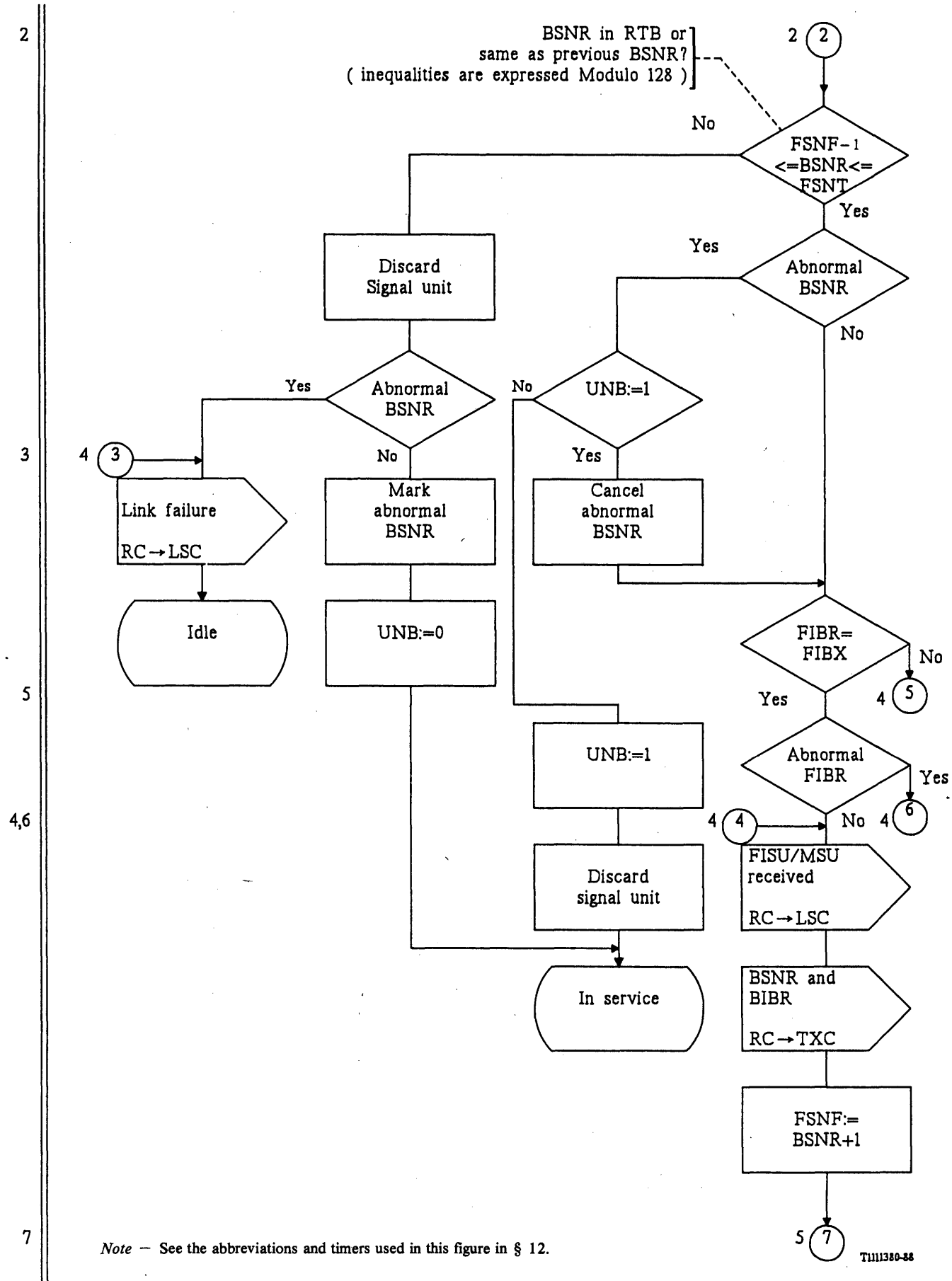
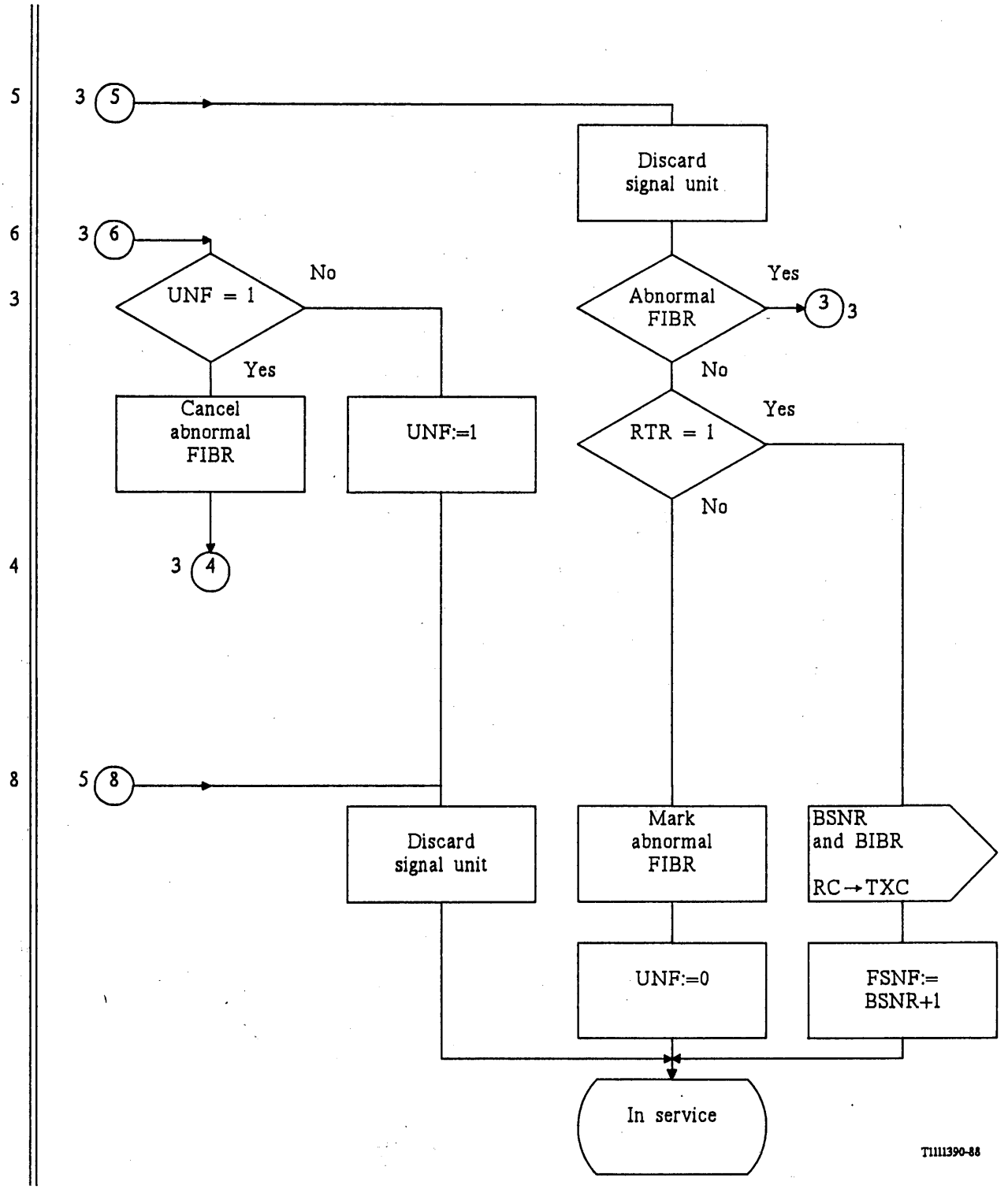



FIGURE 14/Q.703 (sheet 3 of 6)

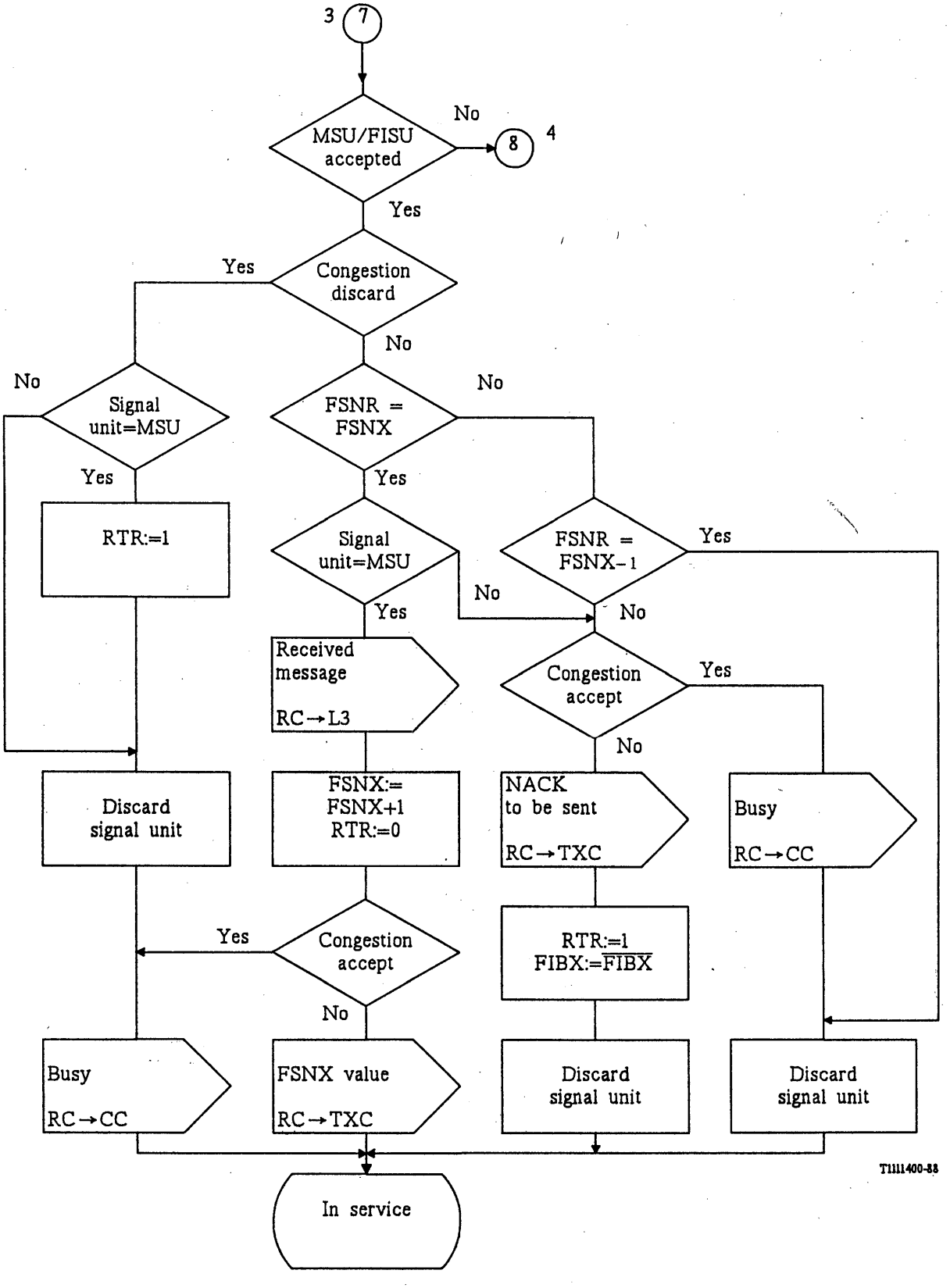
**Basic reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 14/Q.703 (sheet 4 of 6)

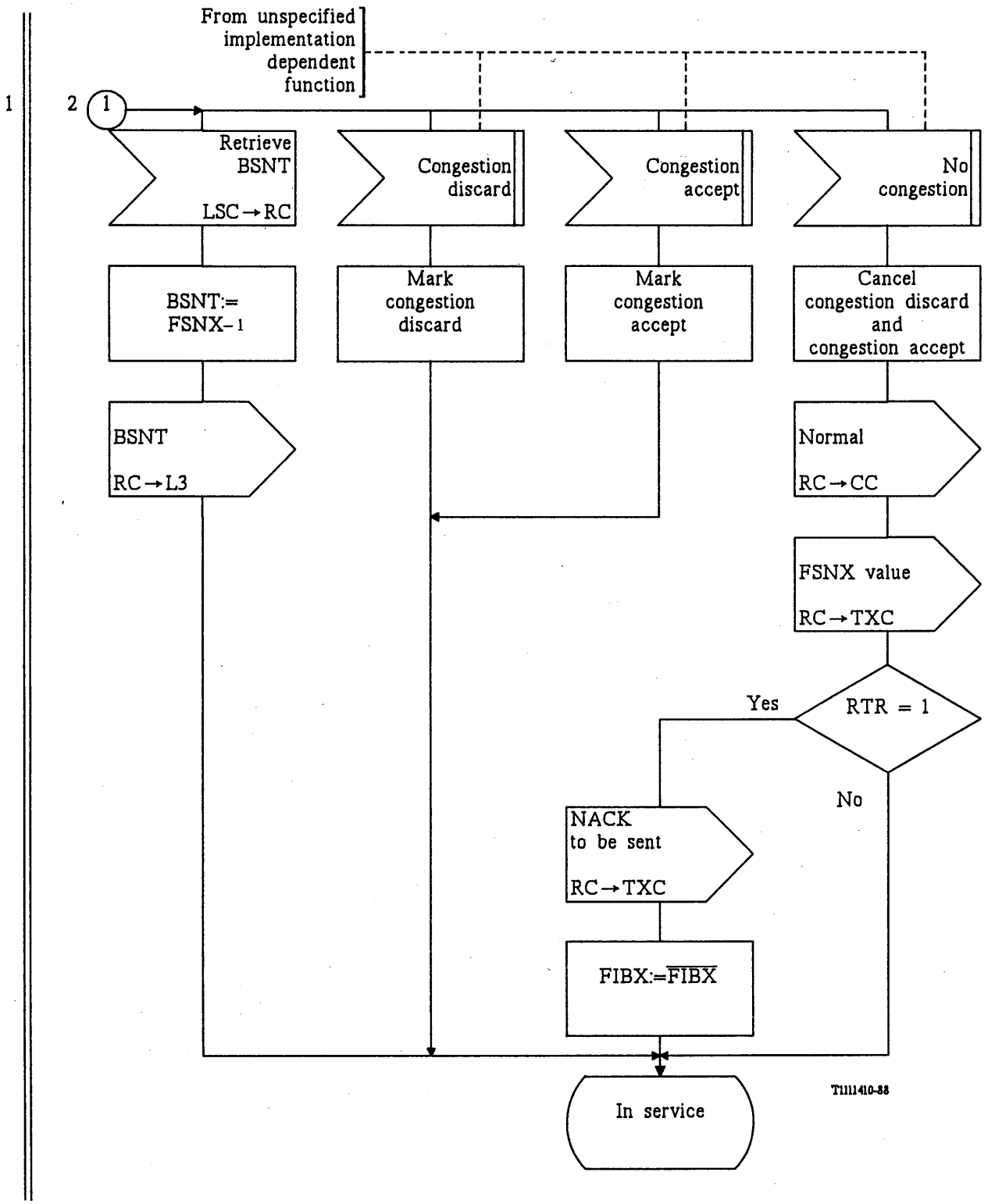
**Basic reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 14/Q.703 (sheet 5 of 6)

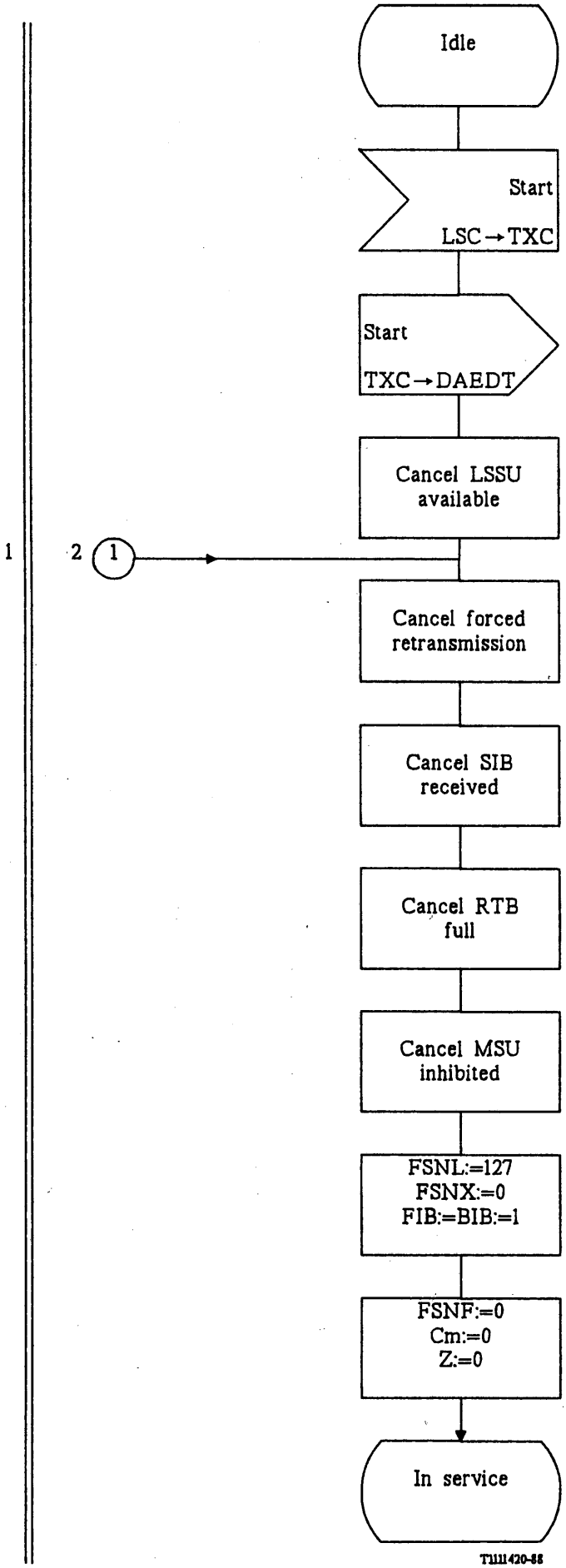
**Basic reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 14/Q.703 (sheet 6 of 6)

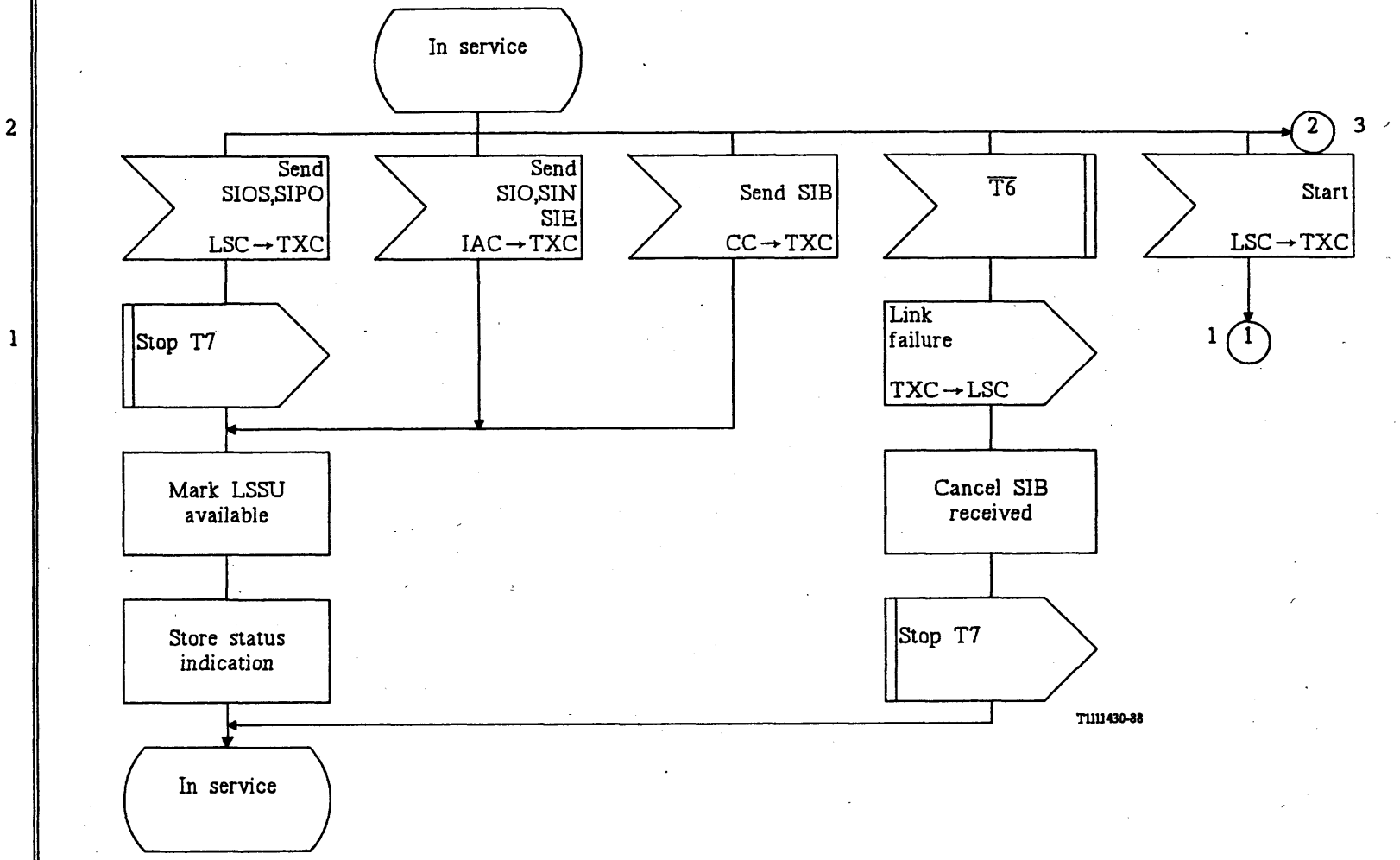
**Basic reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 15/Q.703 (sheet 1 of 6)

**Preventive cyclic retransmission - transmission control**




*Note* — See the abbreviations and timers used in this figure in § 12.

FIGURE 15/Q.703 (sheet 2 of 6)

**Preventive cyclic retransmission - transmission control**

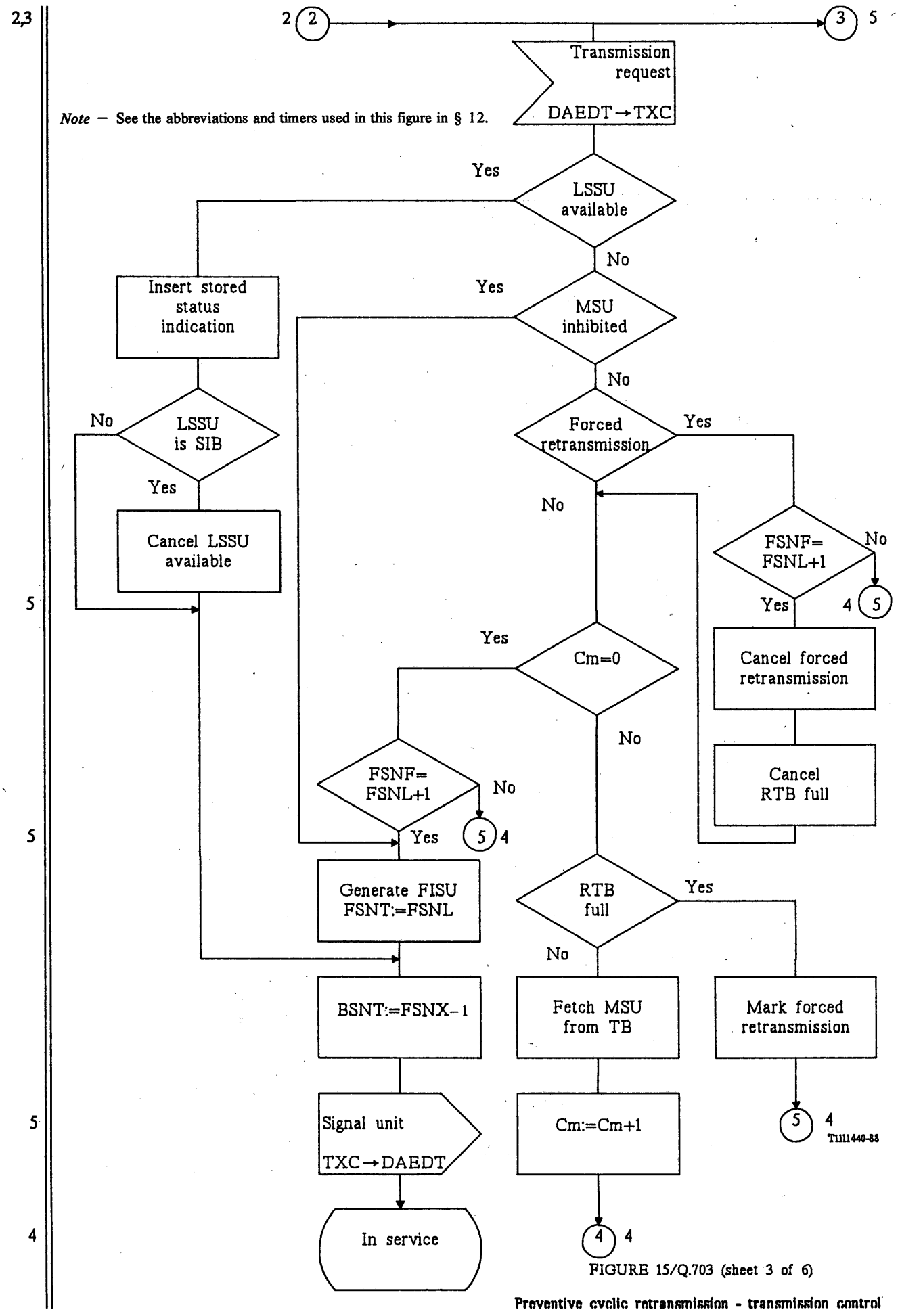
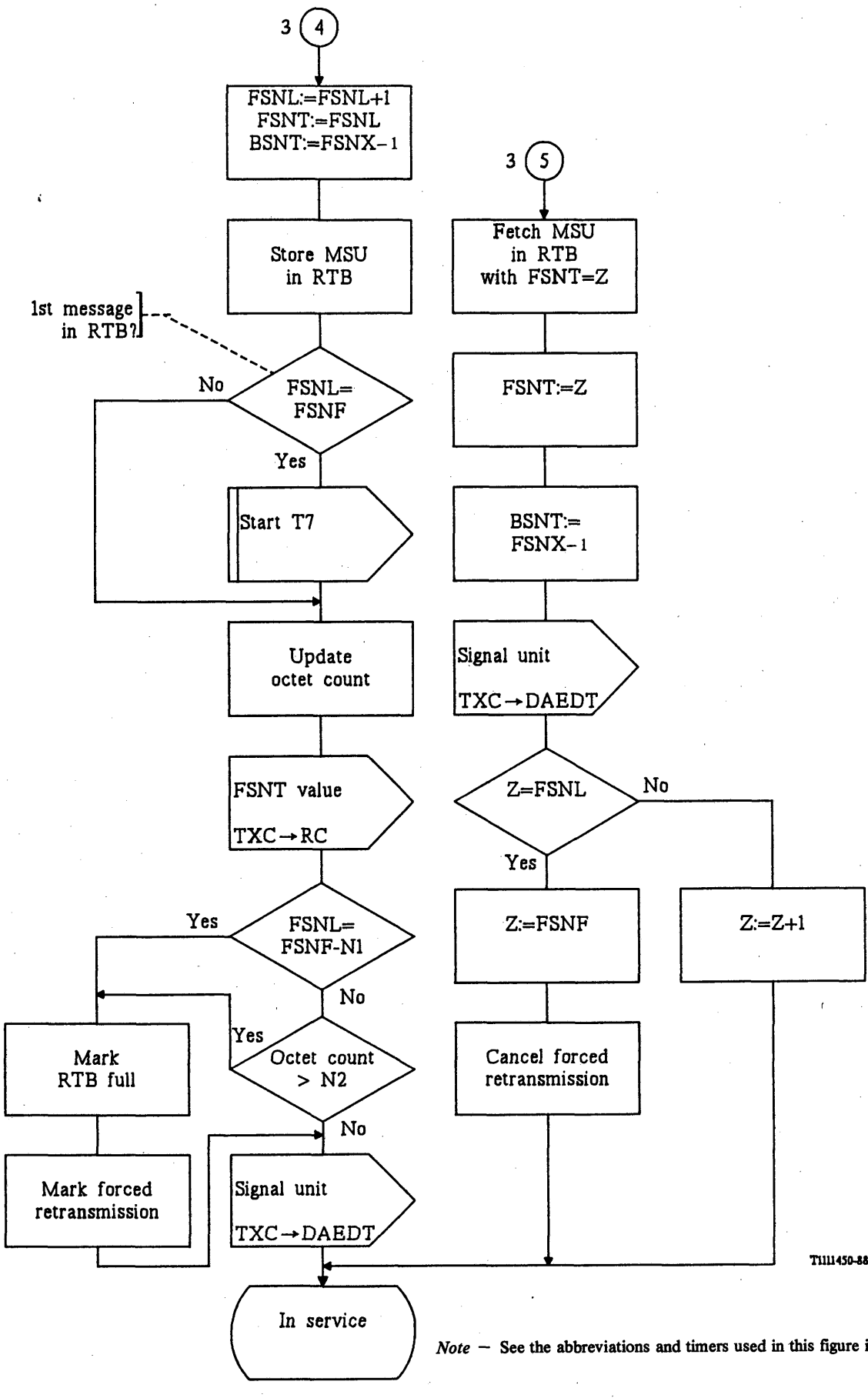



FIGURE 15/Q.703 (sheet 3 of 6)

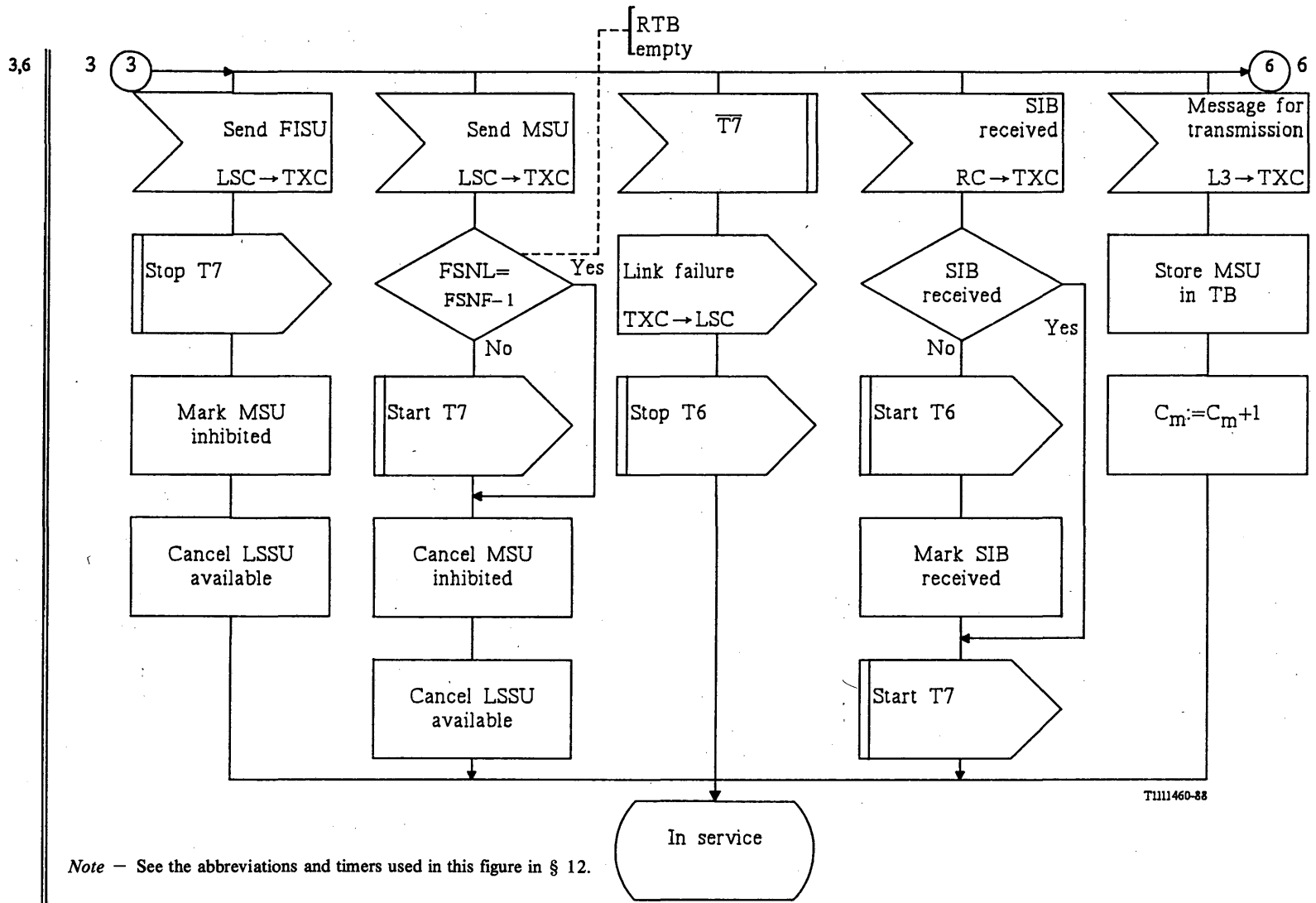
**Preventive cyclic retransmission - transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 15/Q.703 (sheet 4 of 6)

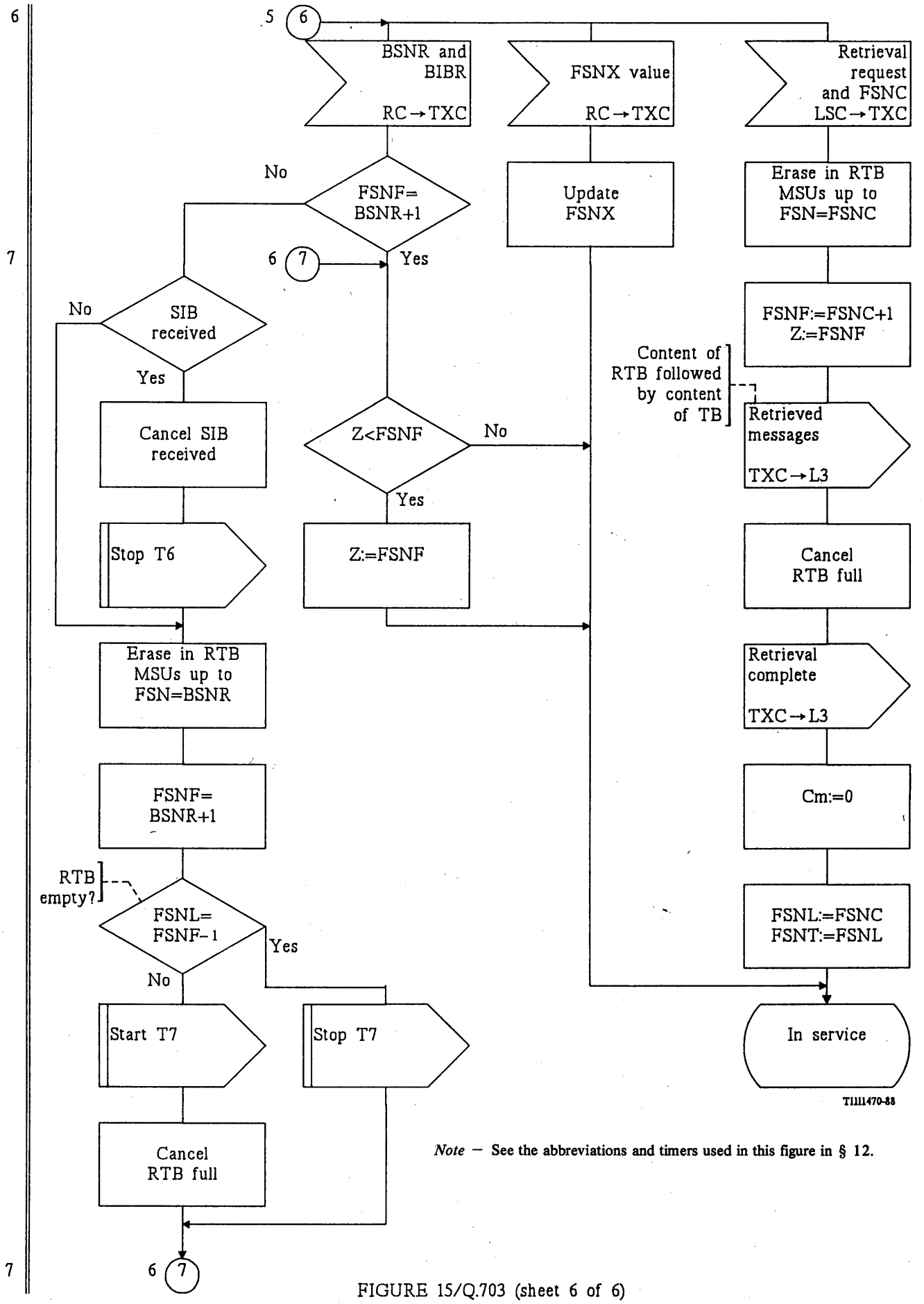
**Preventive cyclic retransmission - transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 15/Q.703 (sheet 5 of 6)

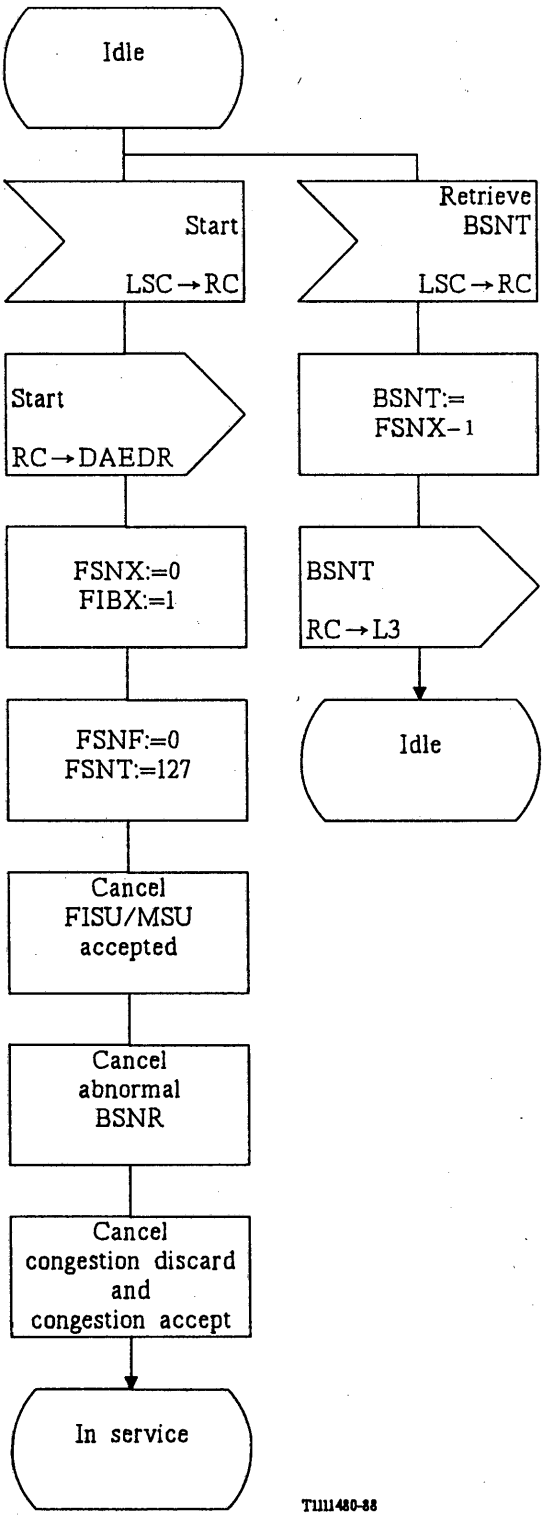
**Preventive cyclic retransmission control - transmission control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 15/Q.703 (sheet 6 of 6)

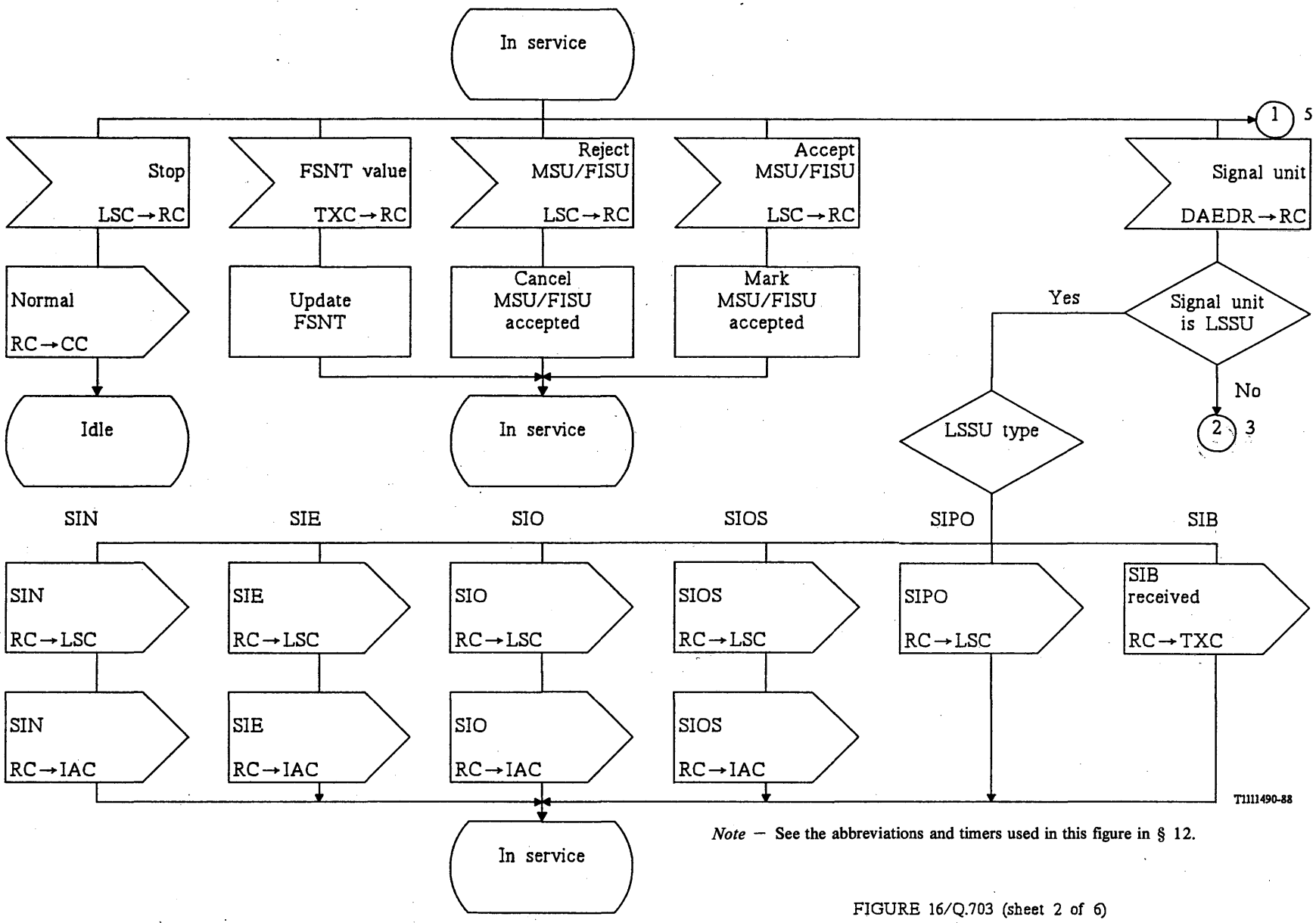
Preventive cyclic retransmission - transmission control




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 16/Q.703 (sheet 1 of 5)

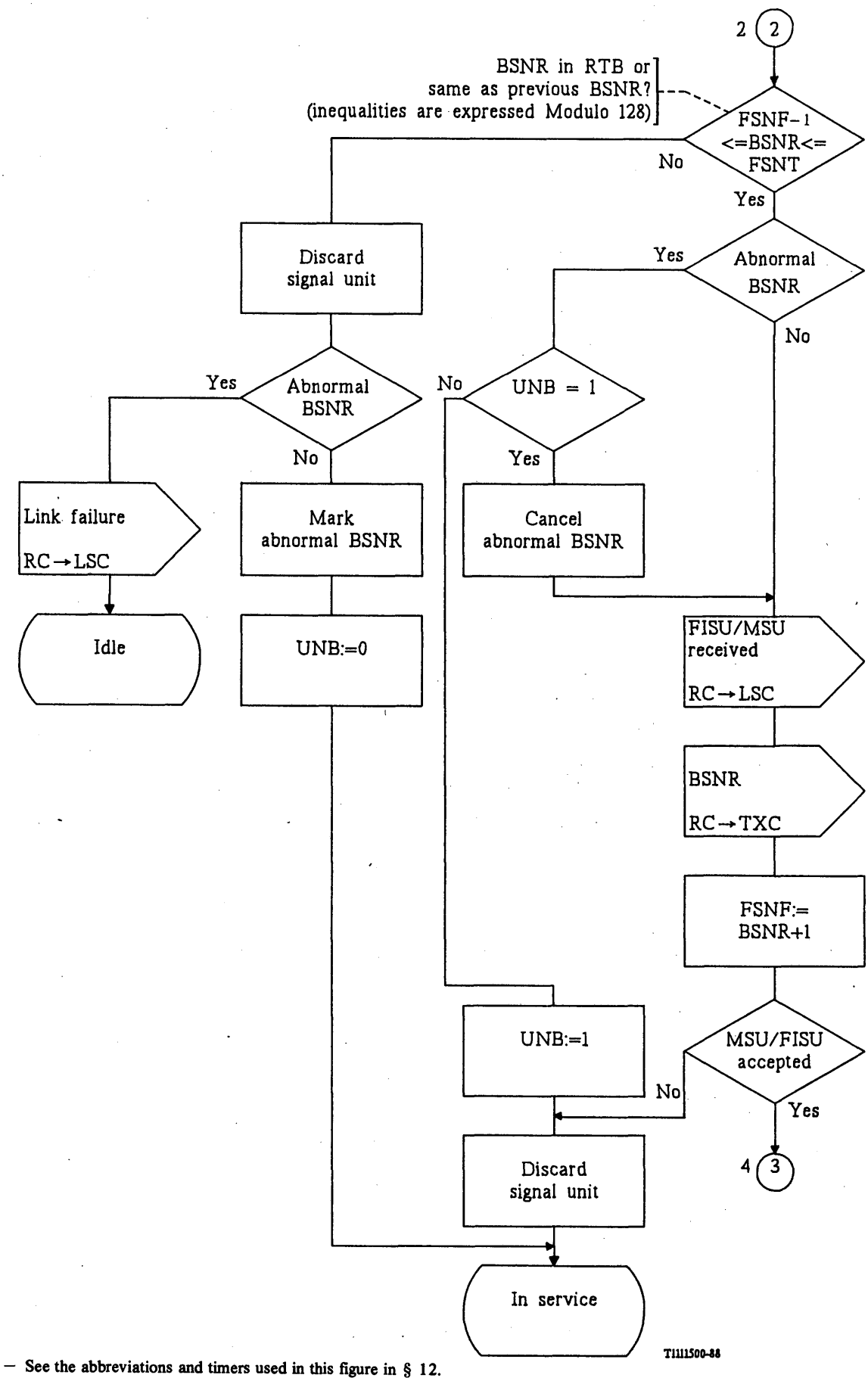
**Preventive cyclic retransmission - reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 16/Q.703 (sheet 2 of 6)

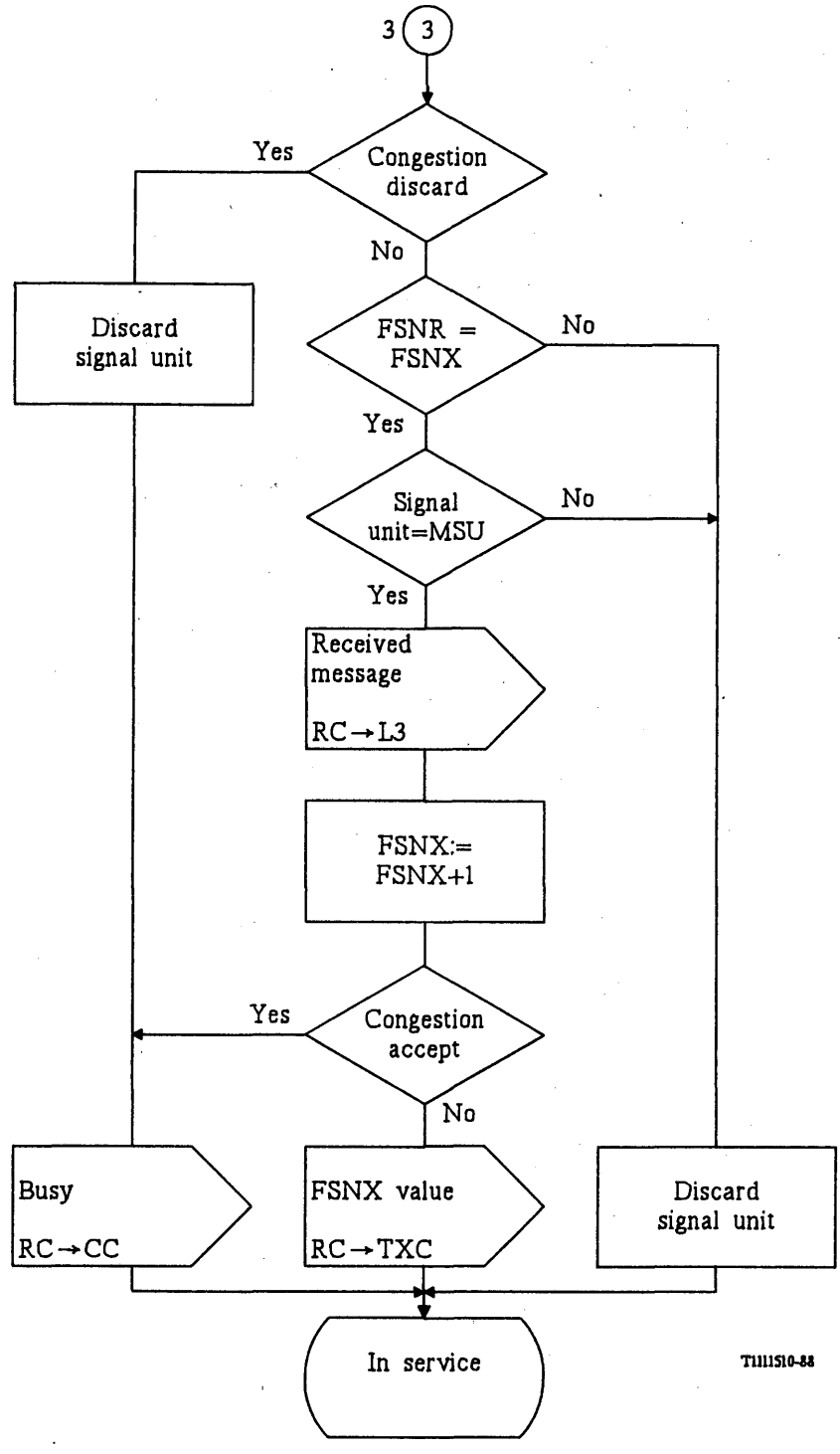
**Preventive cyclic retransmission control - reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 16/Q.703 (sheet 3 of 5)

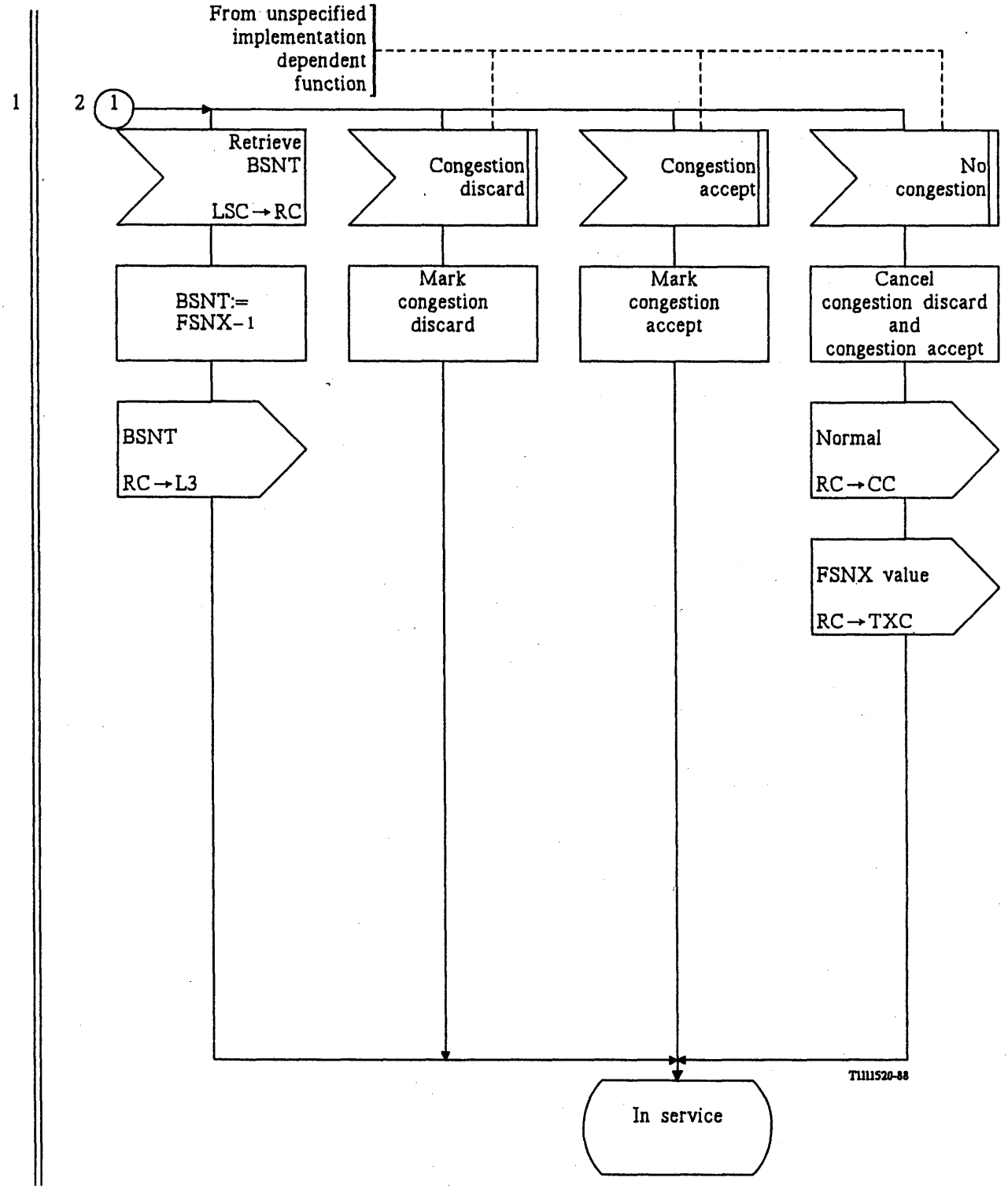
**Preventive cyclic retransmission - reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 16/Q.703 (sheet 4 of 5)

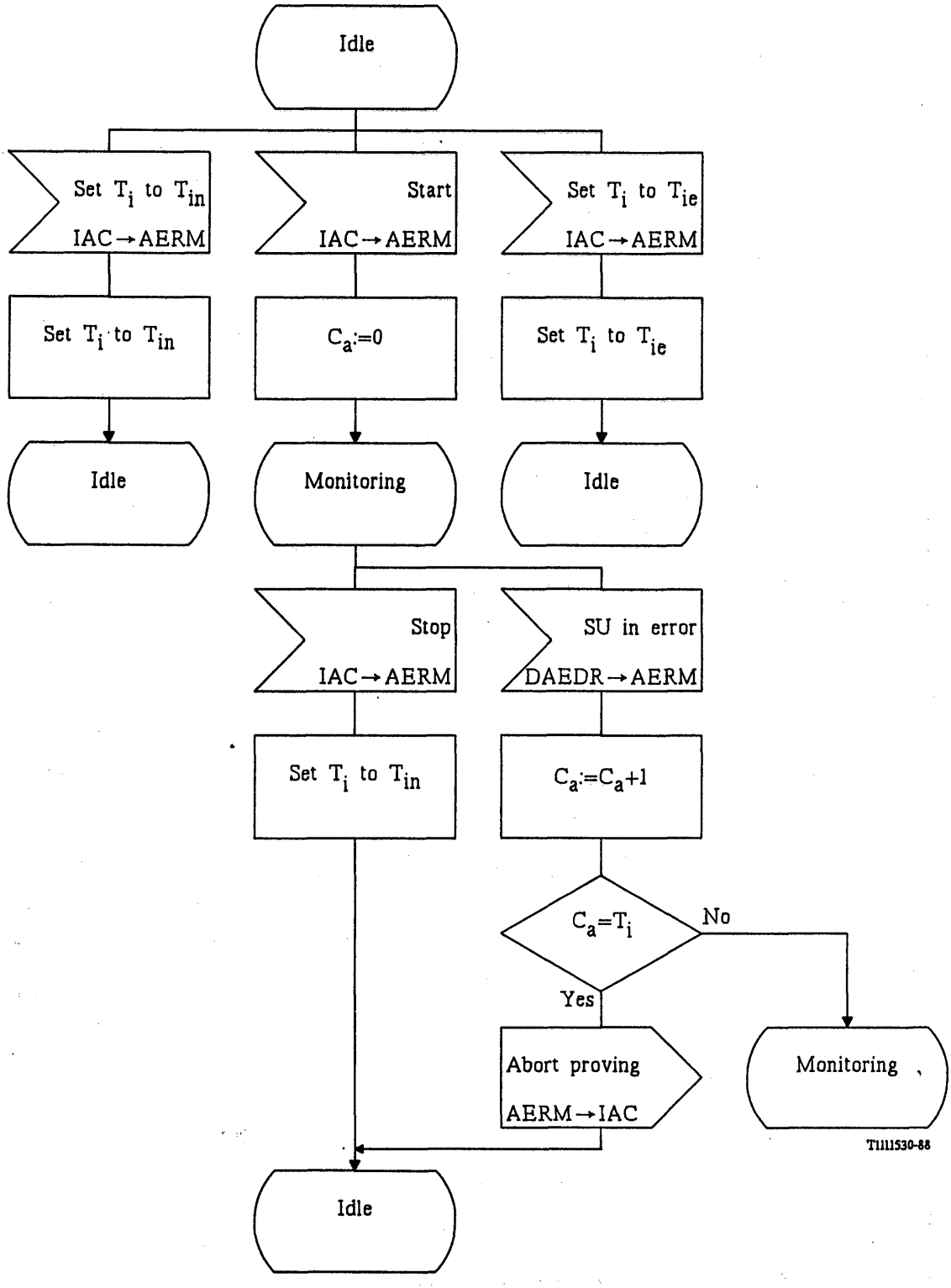
**Preventive cyclic retransmission - reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 16/Q.703 (sheet 5 of 5)

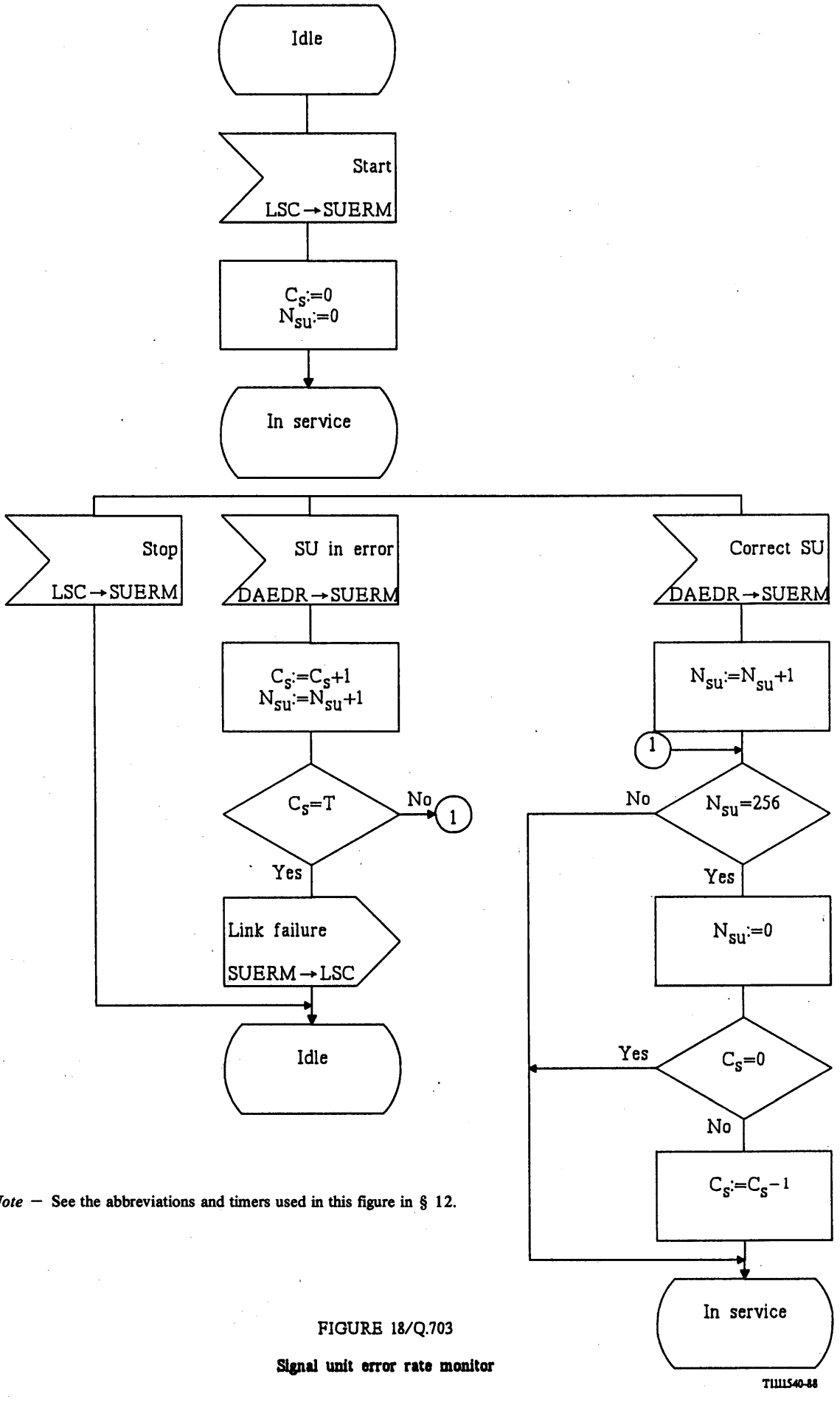
**Preventive cyclic retransmission - reception control**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 17/Q.703

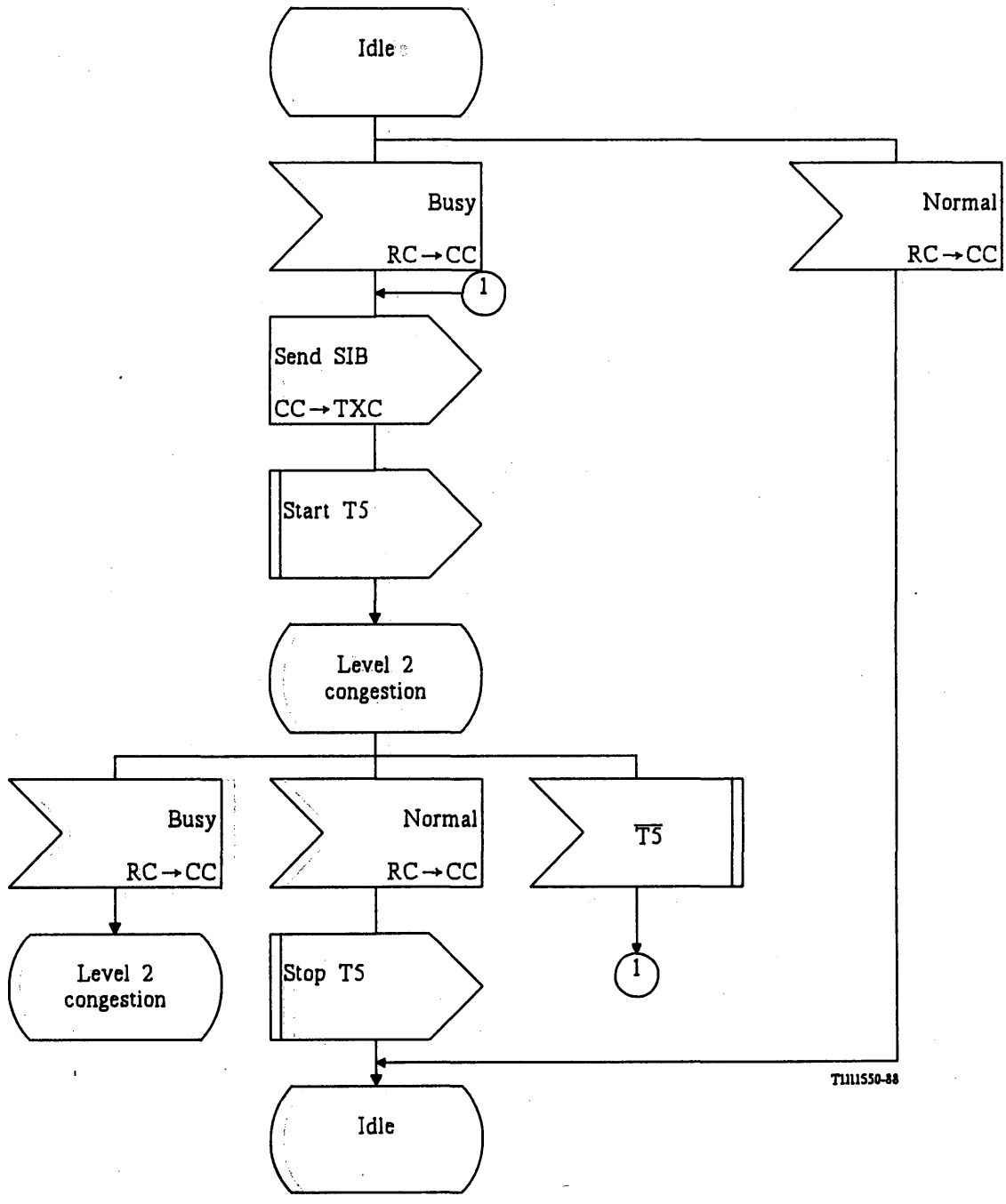
**Alignment error rate monitor**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 18/Q.703

**Signal unit error rate monitor**




*Note* – See the abbreviations and timers used in this figure in § 12.

FIGURE 19/Q.703

**Congestion control**

**Recommendation Q.704**

## SIGNALLING NETWORK FUNCTIONS AND MESSAGES

### 1 Introduction

#### 1.1 *General characteristics of the signalling network functions*

1.1.1 This Recommendation describes the functions and procedures for and relating to the transfer of messages between the signalling points, which are the nodes of the signalling network. Such functions and procedures are performed by the Message Transfer Part at level 3, and therefore they assume that the signalling points are connected by signalling links, incorporating the functions described in Recommendations Q.702 and Q.703. The signalling network functions must ensure a reliable transfer of the signalling messages, according to the requirements specified in Recommendation Q.706, even in the case of the failure of signalling links and signalling transfer points; therefore, they include the appropriate functions and procedures necessary both to inform the remote parts of the signalling network of the consequences of a fault, and to appropriately reconfigure the routing of messages through the signalling network.

1.1.2 According to these principles, the signalling network functions can be divided into two basic categories, namely:

- *signalling message handling*, and
- *signalling network management.*

The signalling message handling functions are briefly summarized in § 1.2, the signalling network management functions in § 1.3. The functional interrelations between these functions are indicated in Figure 1/Q.704.

#### 1.2 *Signalling message handling*

1.2.1 The purpose of the signalling message handling functions is to ensure that the signalling messages originated by a particular User Part at a signalling point (originating point) are delivered to the same User Part at the destination point indicated by the sending User Part.

Depending on the particular circumstances, this delivery may be made through a signalling link directly interconnecting the originating and destination points, or via one or more intermediate signalling transfer points.

1.2.2 The signalling message handling functions are based on the label contained in the messages which explicitly identifies the destination and originating points.

The label part used for signalling message handling by the Message Transfer Part is called the *routing label*; its characteristics are described in § 2.

1.2.3 As illustrated in Figure 1/Q.704, the signalling message handling functions are divided into:

- the *message routing* function, used at each signalling point to determine the outgoing signalling link on which a message has to be sent towards its destination point;
- the *message discrimination* function, used at a signalling point to determine whether or not a received message is destined to the point itself. When the signalling point has the transfer capability and a message is not destined to it, that message has to be transferred to the message routing function;
- the *message distribution* function, used at each signalling point to deliver the received messages (destined to the point itself) to the appropriate User Part.

The characteristics of the message routing, discrimination and distribution functions are described in § 2.

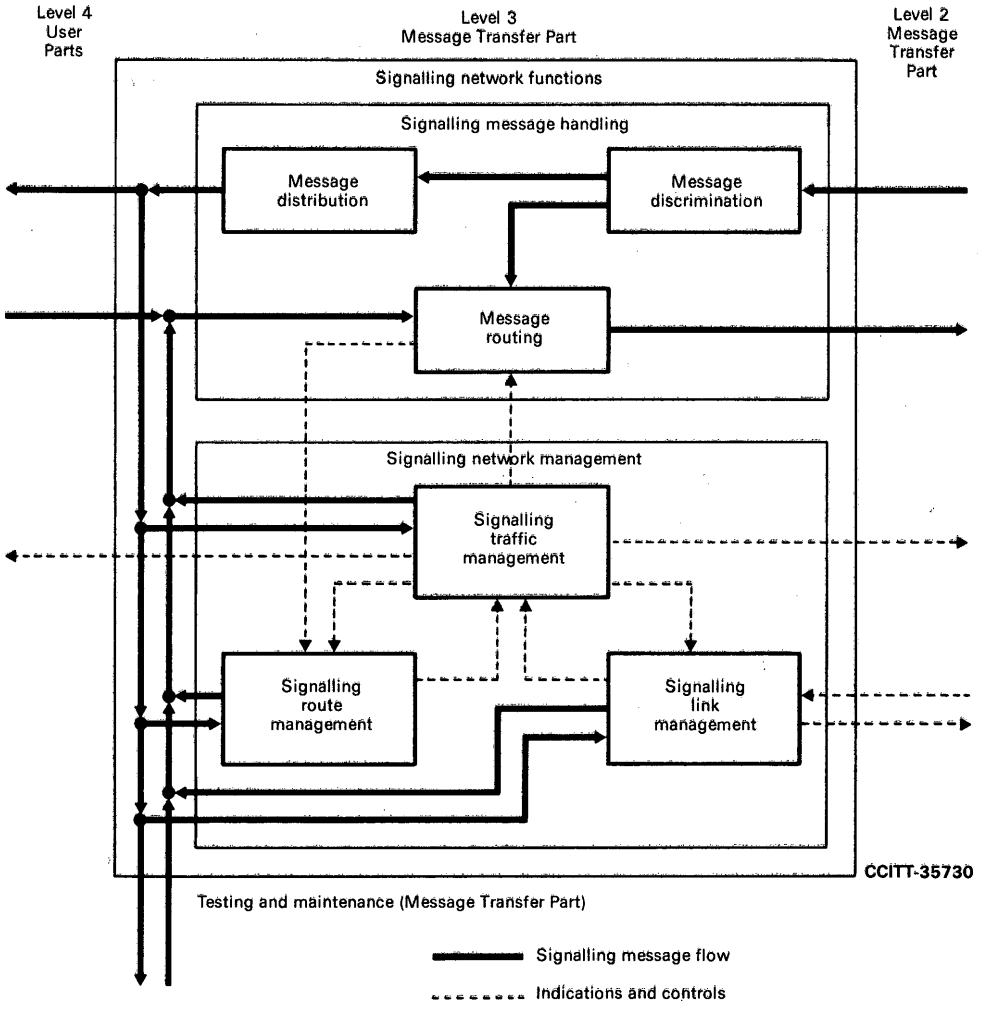



FIGURE 1/Q.704

**Signalling network functions**

## 1.3 *Signalling network management*

1.3.1 The purpose of the signalling network management functions is to provide reconfiguration of the signalling network in the case of failures and to control traffic in case of congestion. Such a reconfiguration is effected by use of appropriate procedures to change the routing of signalling traffic in order to bypass the faulty links or signalling points; this requires communication between signalling points (and, in particular, the signalling transfer points) concerning the occurrence of the failures. Moreover, in some circumstances it is necessary to activate and align new signalling links, in order to restore the required signalling traffic capacity between two signalling points. When the faulty link or signalling point is restored, the opposite actions and procedures take place, in order to reestablish the normal configuration of the signalling network.

1.3.2 As illustrated in Figure 1/Q.704, the signalling network management functions are divided into:

- *signalling traffic management,*
- *signalling link management,* and
- *signalling route management.*

These functions are used whenever an event (such as the failure or restoration of a signalling link) occurs in the signalling network; the list of the possible events and the general criteria used in relation to each signalling network management function are specified in § 3.

1.3.3 §§ 4 to 11 specify the procedures pertaining to signalling traffic management. In particular, the rules to be followed for the modification of signalling routing appear in § 4. The diversion of traffic according to these rules is made, depending on the particular circumstances, by means of one of the following procedures: *changeover, changeback, forced rerouting, controlled rerouting* and *signalling point restart.* They are specified in §§ 5 to 9 respectively. A signalling link may be made unavailable to User Part generated traffic by means of the management inhibiting procedure described in § 10. Moreover, in the case of congestion at signalling points, the signalling traffic management may need to slow down signalling traffic on certain routes by using the *signalling traffic flow control* procedure specified in § 11.

1.3.4 The different procedures pertaining to signalling link management are: *restoration, activation* and *inactivation* of a signalling link, *link set activation* and *automatic allocation* of signalling terminals and signalling data links. These procedures are specified in § 12.

1.3.5 The different procedures pertaining to signalling route management are: the *transfer-prohibited, transfer-allowed, transfer-restricted*[1], *transfer-controlled, signalling-route-set-test* and *signalling-route -set-congestion-test*[1] procedures specified in § 13.

1.3.6 The format characteristics, common to all message signal units which are relevant to the Message Transfer Part, level 3, are specified in § 14.

1.3.7 Labelling, formatting and coding of the signalling network management messages are specified in § 15.

1.3.8 The description of signalling network functions in the form of state transition diagrams according to the CCITT Specification and Description Language (SDL) is given in § 16.

## 2 Signalling message handling

### 2.1 *General*

2.1.1 Signalling message handling comprises message routing, discrimination and distribution functions which are performed at each signalling point in the signalling network.

Message routing is a function concerning the messages to be sent, while message distribution is a function concerning the received messages. The functional relations between message routing and distribution appear in Figure 2/Q.704.

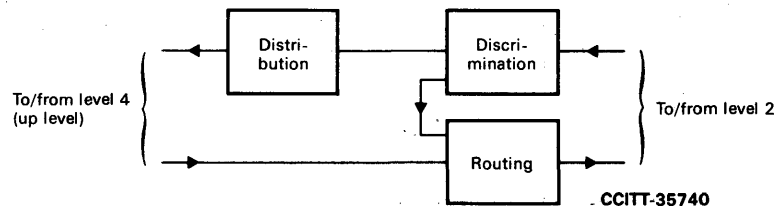



FIGURE 2/Q.704
**Message routing, discrimination and distribution**

[1] National option.

2.1.2 When a message comes from level 4 (or is originated at level 3, in the case of Message Transfer Part level 3 messages), the choice of the particular signalling link on which it has to be sent is made by the message routing function. When two or more links are used at the same time to carry traffic having a given destination, this traffic is distributed among them by the load sharing function, which is a part of the message routing function.

2.1.3 When a message comes from level 2, the discrimination function is activated, in order to determine whether it is destined to another signalling point. When the signalling point has the transfer capability and the received message is not destined to it, the message has to be transmitted on an outgoing link according to the routing function.

2.1.4 In the case that the message is destined to the receiving signalling point, the message distribution function is activated in order to deliver it to the appropriate User Part (or to the local Message Transfer Part level 3 functions).

2.1.5 Message routing, discrimination and distribution are based on the part of the label called the routing label, on the service indicator and, in national networks, also on the network indicator. They can also be influenced by different factors, such as a request (automatic or manual) obtained from a management system.

2.1.6 The position and coding of the service indicator and of the network indicator are described in § 14.2. The characteristics of the label of the messages pertaining to the various User Parts are described in the specification of each separate User Part and in § 15 for the signalling network management messages. The label used for signalling network management messages is also used for testing and maintenance messages (see Recommendation Q.707). Moreover, the general characteristics of the routing label are described in § 2.2.

A description of the detailed characteristics of the message routing function, including load sharing, appears in § 2.3; principles concerning the number of load-shared links appear in Recommendation Q.705.

A description of the detailed characteristics of the message discrimination and distribution functions appears in § 2.4.

2.1.7 In addition to the normal signalling message handling procedures it may, as an option, be possible to prevent the unauthorized use of the message transfer capability of a node. The procedures to be used are implementation-dependent and further information is given in Recommendation Q.705, § 8.

## 2.2 *Routing label*

2.2.1 The label contained in a signalling message, and used by the relevant User Part to identify the particular task to which the message refers (e.g. a telephone circuit), is also used by the Message Transfer Part to route the message towards its destination point.

The part of the message label that is used for routing is called the *routing label* and it contains the information necessary to deliver the message to its destination point.

Normally the routing label is common to all the services and applications in a given signalling network, national or international (however, if this is not the case, the particular routing label of a message is determined by means of the service indicator).

The standard routing label is specified in the following. This label should be used in the international signalling network and is applicable also in national applications.

*Note* – There may be applications using a modified label having the same order and function, but possibly different sizes, of sub-fields as the standard routing label.

2.2.2 The standard routing label has a length of 32 bits and is placed at the beginning of the Signalling Information Field. Its structure appears in Figure 3/Q.704.

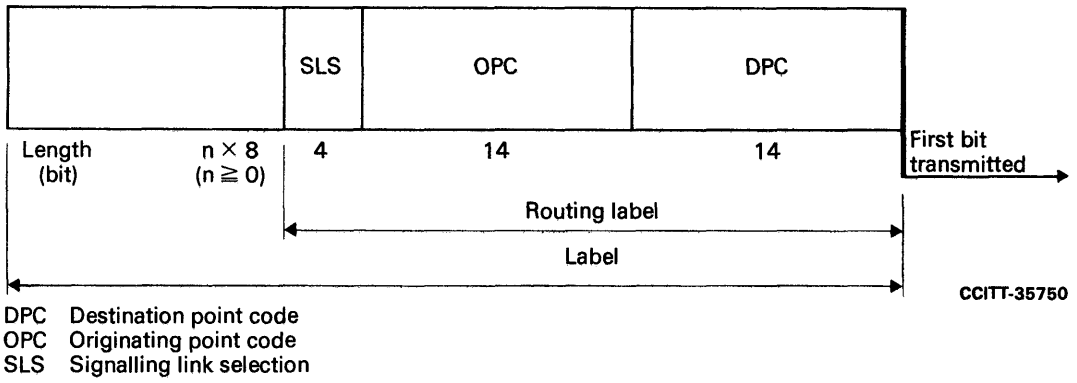



FIGURE 3/Q.704

**Routing label structure**

2.2.3 The *destination point code* (DPC) indicates the destination point of the message. The *originating point code* (OPC) indicates the originating point of the message. The coding of these codes is pure binary. Within each field, the least significant bit occupies the first position and is transmitted first.

A unique numbering scheme for the coding of the fields will be used for the signalling points of the international network, irrespective of the User Parts connected to each signalling point.

2.2.4 The *signalling link selection* (SLS) field is used, where appropriate, in performing load sharing (see § 2.3). This field exists in all types of messages and always in the same position. The only exception to this rule is some Message Transfer Part level 3 messages (e.g., the changeover order), for which the message routing function in the signalling point of origin of the message is not dependent on the field: in this particular case the field does not exist as such, but it is replaced by other information (e.g., in the case of the changeover order, the identity of the faulty link).

In the case of circuit related messages of the TUP, the field contains the least significant bits of the circuit identification code (or bearer identification code, in the case of the Data User Part), and these bits are not repeated elsewhere. In the case of all other User Parts, the SLS is an independent field in accordance with the criteria stated in § 2.2.5.

In the case of Message Transfer Part level 3 messages, the signalling link selection field exactly corresponds to the *signalling link code* (SLC) which indicates the signalling link between the destination point and originating point to which the message refers.

2.2.5 From the rule stated in § 2.2.4 above, it follows that the signalling link selection of messages generated by any User Parts will be used in the load sharing mechanism. As a consequence, in the case of User Parts which are not specified (e.g., transfer of charging information) but for which there is the requirement to maintain the order of transmission of the messages, the field should be coded with the same value for all messages belonging to the same transaction, sent in a given direction.

2.2.6 The above principles should also apply to modified label structures that may be used nationally.

## 2.3 *Message routing function*

2.3.1 The message routing function is based on information contained in the routing label, namely on the destination point code and on the signalling link selection field; moreover, in some circumstances the service indicator may also need to be used for routing purposes.

*Note* – A possible case for the use of the service indicator is that which would arise from the use of messages supporting the signalling route management function (i.e. transfer-prohibited, transfer-allowed and signalling-route-set-messages) referring to a destination more restrictive than a single signalling point (e.g., an individual User Part) (see § 13). Some specific routing may be required for the MTP Testing User Part (for further study).

The number of such cases should be kept to a minimum in order to apply the same routing criteria to as many User Parts as possible.

Each signalling point will have routing information that allows it to determine the signalling link over which a message has to be sent on the basis of the destination point code and signalling link selection field and, in some cases, of the network indicator (see § 2.4.3). Typically the destination point code is associated with more than one signalling link that may be used to carry the message; the selection of the particular signalling link is made by means of the signalling link selection field, thus effecting load sharing.

2.3.2 Two basic cases of load sharing are defined, namely:

a) load sharing between links belonging to the same link set,

b) load sharing between links not belonging to the same link set.

A load sharing collection of one or more link sets is called a combined link set.

The capability to operate in load sharing according to both these cases is mandatory for any signalling point in the international network.

In case a), the traffic flow carried by a link set is shared (on the basis of the signalling link selection field) between different signalling links belonging to the link set. An example of such a case is given by a link set directly interconnecting the originating and destination points in the associated mode of operation, such as represented in Figure 4/Q.704.

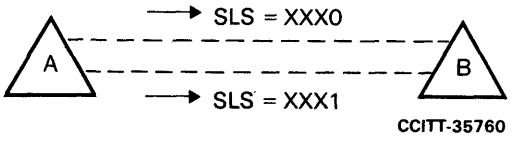



FIGURE 4/Q.704

**Example of load sharing within a link set**

In case b) traffic relating to a given destination is shared (on the basis of the signalling link selection field) between different signalling links not belonging to the same link set, such as represented in Figure 5/Q.704. The load sharing rule used for a particular signalling relation may or may not apply to all the signalling relations which use one of the signalling links involved (in the example, traffic destined to B is shared between signalling links DE and DF with a given signalling link selection field assignment, while that destined to C is sent only on link DF, due to the failure of link EC).

As a result of the message routing function, in normal conditions all the messages having the same routing label (e.g., call set-up messages related to a given circuit) are routed via the same signalling links and signalling transfer points.

Principles relating to the number of load-shared links appear in Recommendation Q.705.

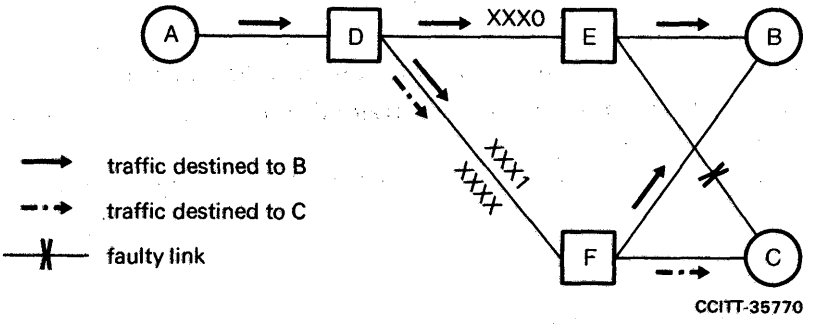



FIGURE 5/Q.704

**Example of load sharing between link sets**

2.3.3 The routing information mentioned in § 2.3.1 should be appropriately updated when some event happens in the signalling network, which is relevant to the concerned signalling point (e.g., failure of a signalling link or unavailability of a signalling route). The updating of the routing information is made according to the particular event (see § 3) and to the signalling routing modification rules specified in § 4. If a signalling transfer point receives a message for destination point code which according to the routing information does not exist, the message is discarded and an indication is given to a management system.

2.3.4 *Handling of level 3 messages*

2.3.4.1 Messages not related to a signalling link have the signalling link code 0000 (e.g., transfer prohibited and transfer allowed). They are handled in accordance with the normal routing function, where the signalling link code (SLC) is used in the same way as SLS for load sharing.

2.3.4.2 Messages related to a signalling link should be subdivided into 2 groups:

a) Messages that are to be transmitted over a specific signalling link (e.g., changeback declaration (see § 6) and signalling link test messages (Recommendation Q.707)), where a special routing function must ensure that these messages are transmitted exclusively over a particular signalling link.

b) Messages that must not be transmitted over a specific signalling link (e.g., changeover messages and emergency changeover messages (see § 5)), whose transmission over the signalling link defined by the SLC contained in the label must be avoided.

2.3.5 *Handling of messages under signalling link congestion*

2.3.5.1 In the international signalling network, congestion priorities of messages are only assigned and the decision to discard under congestion is only made within each User Part. Message discard will only occur in the MTP should there be an extreme resource limitation (for the MTP there is no congestion priority).

In national signalling networks, each message may be assigned by its generating User Part a congestion priority. This is used by the MTP to determine whether or not a message should be discarded under signalling link congestion. $N + 1$ levels of congestion priority ($0 \leqslant N \leqslant 3$) levels are accommodated in the signalling network, with 0 being the lowest and $N$ the highest.

In national signalling networks using more than one congestion priority, the highest priority is assigned to signalling network management messages.

2.3.5.2 *In national signalling networks using multiple congestion priorities*

When a signalling link has been selected for transmitting a message, comparison of the congestion priority of the message is made with the congestion status of the selected signalling link (see § 3.8). If the congestion priority is not less than the signalling link congestion status, that message is transmitted using the selected signalling link.

Otherwise, a transfer-controlled message is sent in response as specified in § 13.7. In this case, the disposition of the concerned message is determined according to the following criteria:

i) If the congestion priority of the message is greater than or equal to the signalling link discard status, the message is transmitted.

ii) If the congestion priority of the message is less than the signalling link discard status, the message is discarded.

2.4 *Message discrimination and distribution functions*

2.4.1 The routing criteria and load sharing method described in § 2.3 imply that a signalling point, sending messages pertaining to a given signalling transaction on a given link, should be able to receive and process messages pertaining to that transaction, e.g., in response to the sent ones, coming from any (but only one) link.

The destination point code field of the received message is examined by the discrimination function in order to determine whether or not it is destined to the receiving signalling point. When the receiving signalling point has the transfer capability and the message is not destined to it, that message has to be directed to the routing function, as described in the previous sections, in order to be sent on the appropriate outgoing link towards the message destination point.

When a signalling transfer point detects that a received message cannot be delivered to its destination point, it sends in response a transfer-prohibited message as specified in § 13.2.

2.4.2 If the destination point code of the message identifies the receiving signalling point, the service indicator is examined by the message distribution function and the message is delivered to the corresponding User Part (or to the Message Transfer Part level 3).

Should a User become unavailable (User unavailability is an implementation dependent notion), this is detected by the MTP. Whether the distribution marked accordingly is implementation dependent.

When the distribution function detects that a received message cannot be delivered to the required User (implementation dependent criteria), a User Part Unavailable message should be returned to the originating end on a response basis. In the originating signalling point, the relevant User Part should be informed via an MTP-STATUS primitive. A mandatory parameter Cause is included in the MTP status indication with two possible values:

- Signalling Network Congestion,
- User Part Unavailability.

The User Part should reduce its traffic in an appropriate manner and take specific actions.

2.4.3 In the case of a signalling point handling both international and national signalling traffic (e.g., an international gateway exchange), the network indicator is also examined in order to determine the relevant numbering scheme (international or national) and possibly the label structure. Moreover, within a national network, the network indicator may be examined to discriminate between different label structures or between different signalling point numbering if dependent on the network levels (see § 14.2).

## 3 Signalling network management

### 3.1 *General*

3.1.1 The signalling network management functions provide the actions and procedures required to maintain signalling service, and to restore normal signalling conditions in the event of disruption in the signalling network, either in signalling links or at signalling points. The disruption may be in the form of complete loss of a signalling link or a signalling point, or in reduced accessibility due to congestion. For example, in the case of a link failure, the traffic conveyed over the faulty link should be diverted to one or more alternative links. The link failure may also result in unavailable signalling routes and this, in turn, may cause diversion of traffic at other signalling points in the signalling network (i.e., signalling points to which no faulty links are connected).

3.1.2 The occurrence of, or recovery from failures or congestion generally results in a change of the status of the affected signalling link(s) and route(s). A signalling link may be considered by level 3, either as "available" or "unavailable" to carry signalling traffic; in particular, an available signalling link becomes unavailable if it is recognized as "failed", "deactivated" "blocked[2)]" or "inhibited", and it becomes once again available if it is recognized as "restored", "activated", "unblocked" or "uninhibited" respectively. A signalling route may be considered by level 3 as "available", "restricted" or "unavailable" too. A signalling point may be "available" or "unavailable". A signalling route set may be "congested" or "uncongested". The detailed criteria for the determination of the changes in the status of signalling links, routes and points are described in §§ 3.2, 3.4 and 3.6 respectively.

---

[2)] The "blocked" condition arises when the unavailability of a signalling link does not depend on a failure in the link itself, but on other causes, such as a "processor outage" condition in a signalling point.

3.1.3 Whenever a change in the status of a signalling link, route or point occurs, the three different signalling network management functions (i.e., signalling traffic management, link management and route management) are activated, when appropriate, as follows:

a) The signalling traffic management function is used to divert signalling traffic from a link or route to one or more different links or routes, to restart a signalling point, or to temporarily slow down signalling traffic in the case of congestion at a signalling point; it comprises the following procedures:
   - changeover (see § 5),
   - changeback (see § 6),
   - forced rerouting (see § 7),
   - controlled rerouting (see § 8),
   - signalling point restart (see § 9),
   - management inhibiting (see § 10),
   - signalling traffic flow control (see § 11).

b) The signalling link management function is used to restore failed signalling links, to activate idle (not yet aligned) links and to deactivate aligned signalling links; it comprises the following procedures (see § 12):
   - signalling link activation, restoration and deactivation,
   - link set activation,
   - automatic allocation of signalling terminals and signalling data links.

c) The signalling route management function is used to distribute information about the signalling network status, in order to block or unblock signalling routes; it comprises the following procedures:
   - transfer-controlled procedure (see §§ 13.6, 13.7 and 13.8),
   - transfer-prohibited procedure (see § 13.2),
   - transfer-allowed procedure (see § 13.3),
   - transfer-restricted procedure (see § 13.4),
   - signalling-route-set-test procedure (see § 13.5),
   - signalling-route-set-congestion test procedure (see § 13.9).

3.1.4 An overview of the use of the procedures relating to the different management functions on occurrence of the link, route and point status changes is given in §§ 3.3, 3.5 and 3.7 respectively.

## 3.2 *Status of signalling links*

3.2.1 A signalling link is always considered by level 3 in one of two possible major states: available and unavailable. Depending on the cause of unavailability, the unavailable state can be subdivided into seven possible cases as follows (see also Figure 6/Q.704):

- unavailable, failed or inactive,
- unavailable, blocked,
- unavailable (failed or inactive) and blocked,
- unavailable, inhibited,
- unavailable, inhibited and (failed or inactive),
- unavailable, inhibited and blocked,
- unavailable, (failed or inactive), blocked and inhibited.

The concerned link can be used to carry signalling traffic only if it is available except possibly for certain classes of test and management messages. Eight possible events can change the status of a link: signalling link failure, restoration, deactivation, activation, blocking, unblocking, inhibiting and uninhibiting; they are described in §§ 3.2.2 to 3.2.9.

3.2.2 *Signalling link failure*

A signalling link (in service or blocked, see § 3.2.6) is recognized by level 3 as failed when:

a) A link failure indication is obtained from level 2. The indication may be caused by:
   - intolerably high signal unit error rate (see Recommendation Q.703, § 10);
   - excessive length of the realignment period (see Recommendation Q.703, §§ 4.1 and 7);
   - excessive delay of acknowledgements (see Recommendation Q.703, §§ 5.3 and 6.3);
   - failure of signalling terminal equipment;
   - two out of three unreasonable backward sequence numbers or forward indicator bits (see Recommendation Q.703, §§ 5.3 and 6.3);
   - reception of consecutive link status signal units indicating out of alignment, out of service, normal or emergency terminal status (see Recommendation Q.703, § 1.7);
   - excessive periods of level 2 congestion (see Recommendation Q.703, § 9).

   The first two conditions are detected by the *signal unit error rate monitor* (see Recommendation Q.703, § 10).

b) A request (automatic or manual) is obtained from a management or maintenance system.

Moreover a signalling link which is available (not blocked) is recognized by level 3 as failed when a changeover order is received.

3.2.3 *Signalling link restoration*

A signalling link previously failed is restored when both ends of the signalling link have successfully completed an initial alignment procedure (see Recommendation Q.703, § 7).

3.2.4 *Signalling link deactivation*

A signalling link (in service, failed or blocked) is recognized by level 3 as deactivated (i.e., removed from operation) when:

a) a request is obtained from the signalling link management function (see § 12);

b) a request (automatic or manual) is obtained from an external management or maintenance system.

3.2.5 *Signalling link activation*

A signalling link previously inactive is recognized by level 3 as activated when both ends of the signalling link have successfully completed an initial alignment procedure (see Recommendation Q.703, § 7).

3.2.6 *Signalling link blocking*

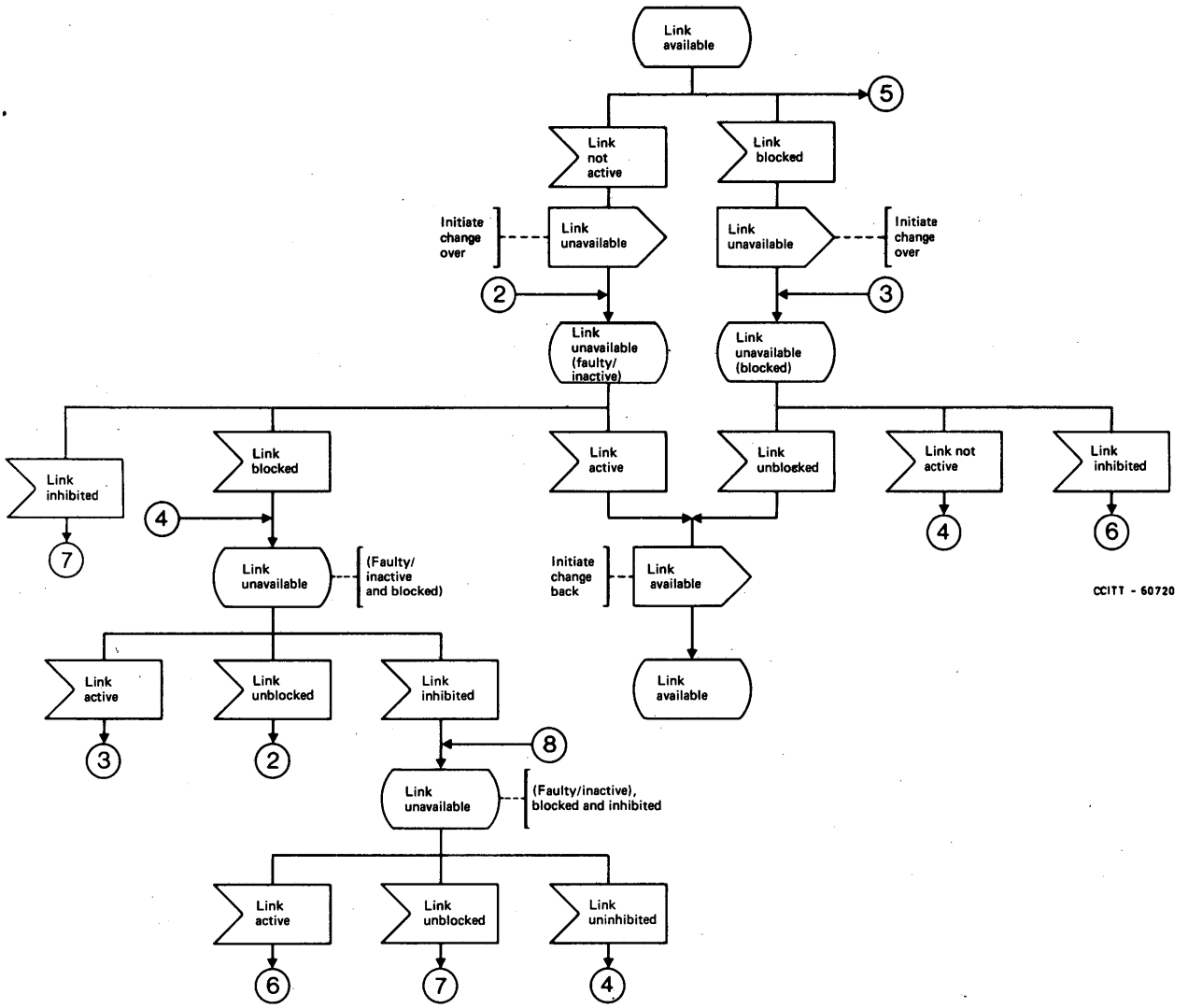
A signalling link (in service, failed or inactive) is recognized as blocked when an indication is obtained from the signalling terminal that a processor outage condition exists at the remote terminal (i.e., link status signal units with processor outage indication are received, see Recommendation Q.703, § 8).

*Note* – A link becomes unavailable when it is failed or deactivated or [(failed or deactivated) and blocked] or inhibited. See Figure 6/Q.704.

3.2.7 *Signalling link unblocking*

A signalling link previously blocked is unblocked when an indication is obtained from the signalling terminal that the processor outage condition has ceased at the remote terminal. (Applies in the case when the processor outage condition was initiated by the remote terminal.)

*Note* – A link becomes available when it is restored or activated or unblocked, or [(restored or activated) and (unblocked)] or uninhibited. See Figure 6/Q.704.

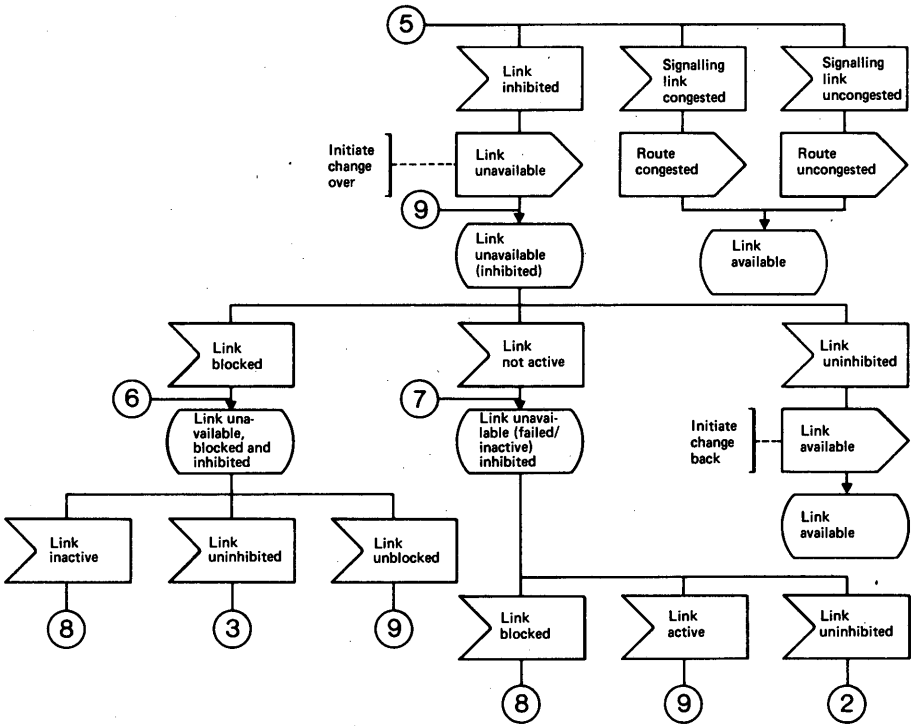



*Signalling link availability*

*Note* – Link not active signal represents both link failure and link deactivation.
Link active signal represents both link restoration and link activation.

FIGURE 6/Q.704 (sheet 1 of 4)

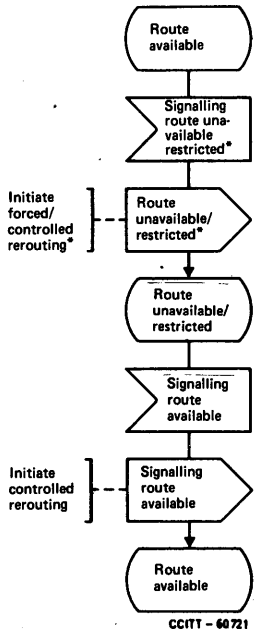
**Signalling traffic management overview diagram**




*Signalling link availability*

FIGURE 6/Q.704 (sheet 2 of 4)

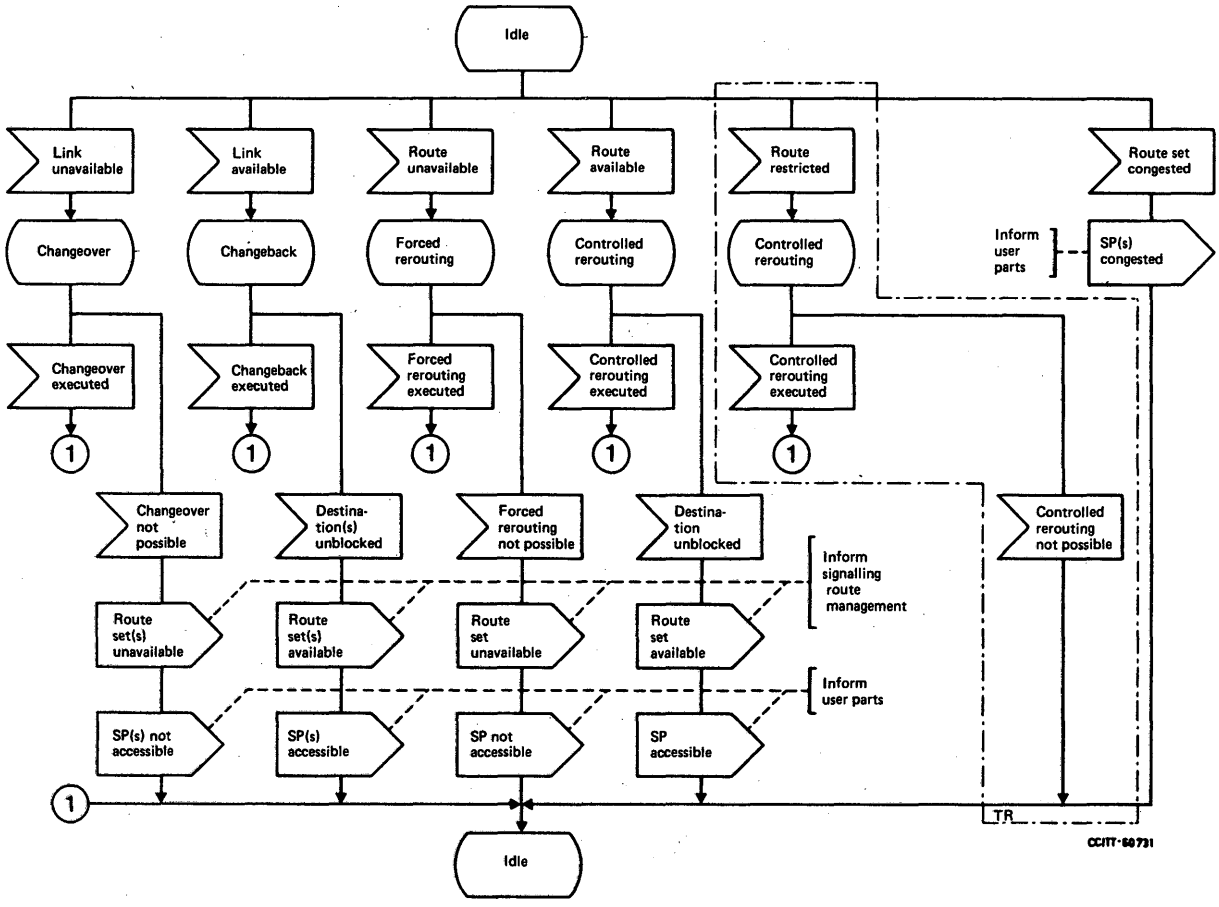
**Signalling traffic management overview diagram**




*Signalling route availability status*

FIGURE 6/Q.704 (sheet 3 of 4)

**Signalling traffic management overview diagram**




*Signalling traffic reconfiguration and flow control*

FIGURE 6/Q.704 (sheet 4 of 4)

**Signalling traffic management overview diagram**

3.2.8 *Signalling link inhibiting*

A signalling link is recognized as inhibited when:

a) an acknowledgement is received from a remote signalling point in response to an inhibit request sent to the remote end by the local signalling link management. Level 3 has marked the link locally inhibited;

b) upon receipt of a request from a remote signalling point to inhibit a link and successful determination that no destination will become inaccessible by inhibiting the link, the link has been marked remotely inhibited by level 3.

3.2.9 *Signalling link uninhibiting*

A signalling link previously inhibited is uninhibited when:

a) a request is received to uninhibit the link from a remote end or from a local routing function;

b) an acknowledgement is received from a remote signalling point in response to an uninhibit request sent to the remote end by the local signalling link management.

3.3 *Procedures used in connection with link status changes*

In § 3.3, the procedures relating to each signalling management function, which are applied in connection with link status changes, are listed. See also Figures 6/Q.704, 7/Q.704 and 8/Q.704. Typical examples of the application of the procedures to the particular network cases appear in Recommendation Q.705.

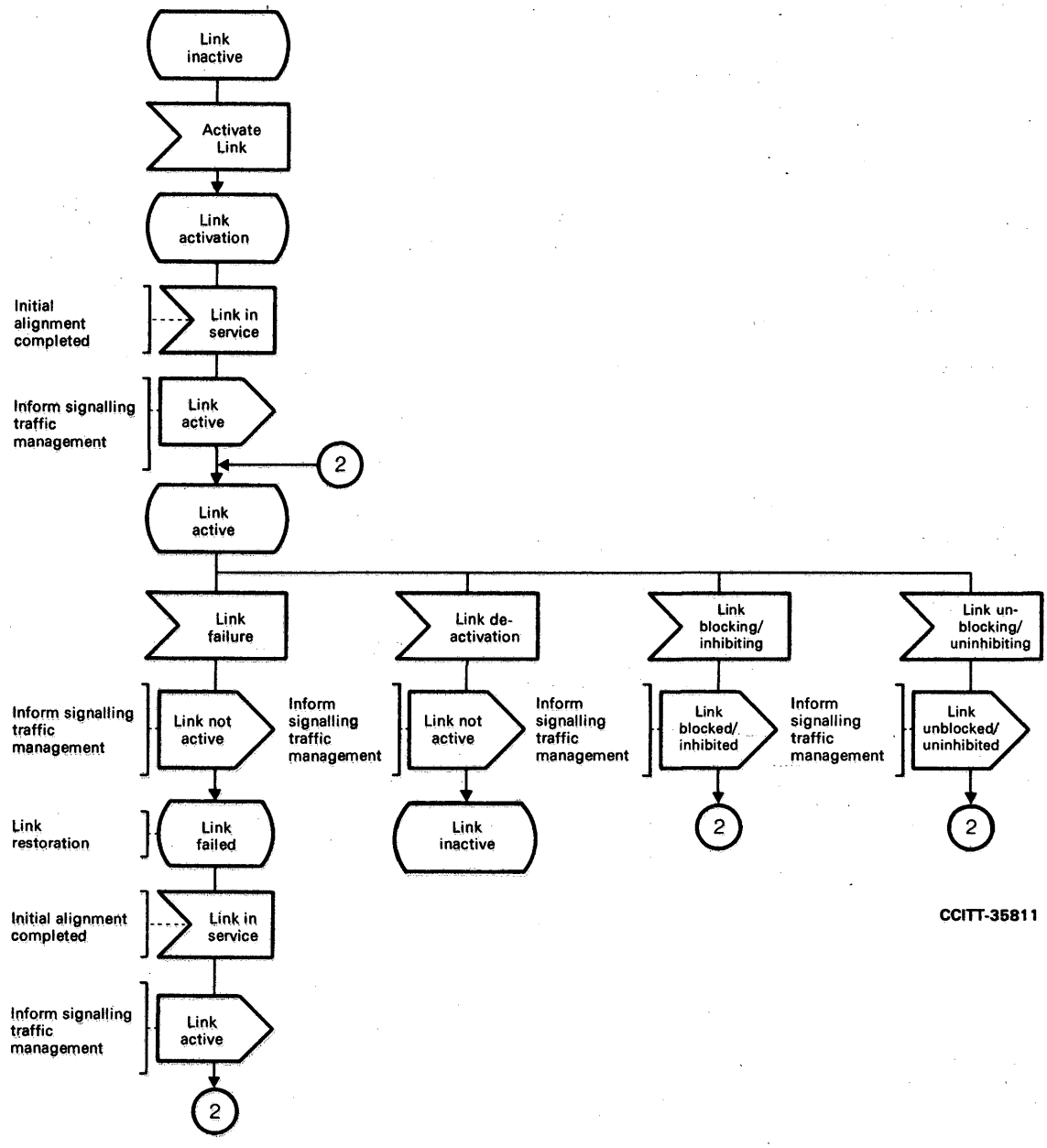



FIGURE 7/Q.704

**Signalling link management overview diagram**

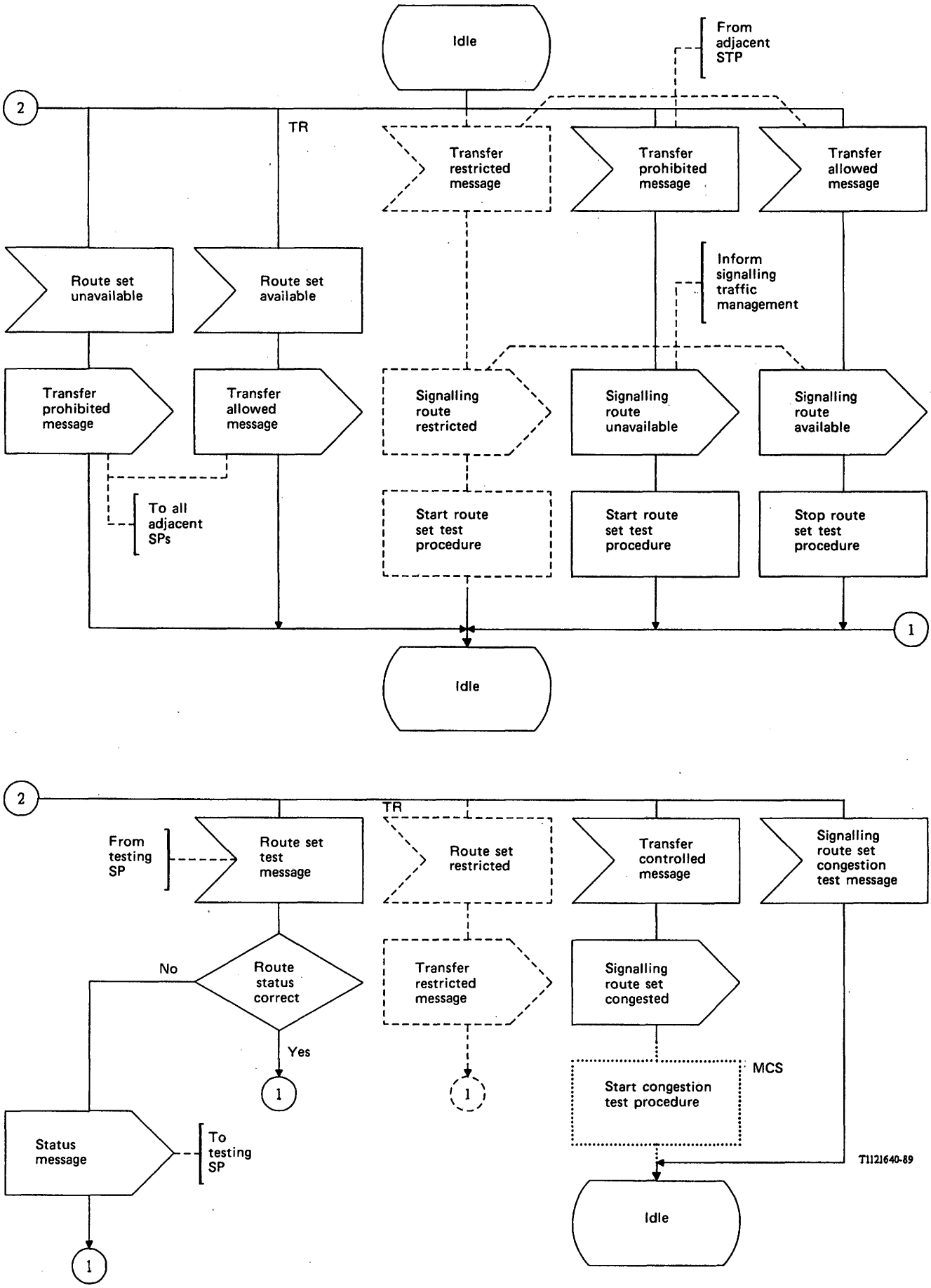



FIGURE 8/Q.704

**Signalling route management overview diagram**

3.3.1 *Signalling link failed*

3.3.1.1 Signalling traffic management: the changeover procedure (see § 5) is applied, if required, to divert signalling traffic from the unavailable link to one or more alternative links with the objective of avoiding message loss, repetition or mis-sequencing; it includes determination of the alternative link or links where the affected traffic can be transferred and procedures to retrieve messages sent over the failed link but not received by the far end.

3.3.1.2 Signalling link management: the procedures described in § 12 are used to restore a signalling link and to make it available for signalling. Moreover, depending on the link set status, the procedures can also be used to activate another signalling link in the same link set to which the unavailable link belongs and to make it available for signalling.

3.3.1.3 Signalling route management: in the case when the failure of a signalling link causes a signalling route set to become unavailable or restricted[3)], the signalling transfer point which can no longer route the concerned signalling traffic applies the transfer-prohibited procedures or transfer-restricted[3)] procedures described in § 13.

3.3.2 *Signalling link restored*

3.3.2.1 Signalling traffic management: the changeback procedure (see § 6) is applied, if required, to divert signalling traffic from one or more links to a link which has become available; it includes determination of the traffic to be diverted and procedures for maintaining the correct message sequence.

3.3.2.2 Signalling link management: the signalling link deactivation procedure (see § 12) is used if, during the signalling link failure, another signalling link of the same link set was activated; it is used to assure that the link set status is returned to the same state as before the failure. This requires that the active link activated during the link failure is deactivated and considered no longer available for signalling.

3.3.2.3 Signalling route management: in the case when the restoration of a signalling link causes a signalling route set to become available, the signalling transfer point which can once again route the concerned signalling traffic applies the transfer-allowed procedures described in § 13.

3.3.3 *Signalling link deactivated*

3.3.3.1 Signalling traffic management: as specified in § 3.3.1.1.

*Note* – The signalling traffic has normally already been removed when signalling link deactivation is initiated.

3.3.3.2 Signalling link management: if the number of active signalling links in the link set to which the deactivated signalling link belongs has become less than the normal number of active signalling links in that link set, the procedures described in § 12 may be used to activate another signalling link in the link set.

3.3.3.3 Signalling route management: as specified in § 3.3.1.3.

3.3.4 *Signalling link activated*

3.3.4.1 Signalling traffic management: as specified in § 3.3.2.1.

3.3.4.2 Signalling link management: if the number of active signalling links in the link set to which the activated signalling link belongs has become greater than the normal number of active signalling links in that link set, the procedures described in § 12 may be used to deactivate another signalling link in the link set.

3.3.4.3 Signalling route management: as specified in § 3.3.2.3.

---

3) National option.

3.3.5 *Signalling link blocked*

3.3.5.1 Signalling traffic management: as specified in § 3.3.1.1.

As a national option, local processor outage may also be applied to the affected signalling link before commencement of the appropriate signalling traffic management option. On completion of that signalling traffic management action, local processor outage is removed from the affected signalling link. No further signalling traffic management will be performed on that affected signalling link until a timer T24 (see § 16.8) has expired or been cancelled, thus allowing time for indications from the remote end to stabilize as it carries out any signalling traffic management of its own.

3.3.5.2 Signalling route management: if the blocking of the link causes a signalling route set to become unavailable or restricted[4)], the signalling transfer point which can no longer route the concerned signalling traffic applies the transfer-prohibited or transfer-restricted[4)] procedures described in § 13.

3.3.6 *Signalling link unblocked*

3.3.6.1 Signalling traffic management: the actions will be the same as in § 3.3.2.1.

3.3.6.2 Signalling route management: if the link unblocked causes a signalling route set to become available, the signalling transfer point which can once again route the signalling traffic in that route set applies the transfer-allowed procedures described in § 13.

3.3.7 *Signalling link inhibited*

3.3.7.1 Signalling traffic management: as specified in § 3.3.1.1.

3.3.7.2 Signalling link management: as specified in § 3.3.3.2.

3.3.8 *Signalling link uninhibited*

3.3.8.1 Signalling traffic management: as specified in § 3.3.2.1.

3.3.8.2 Signalling link management: as specified in § 3.3.4.2.

3.3.8.3 Signalling route management: if the link uninhibited causes a signalling route set to become available, the signalling transfer point which can once again route the signalling traffic in that route set applies the transfer-allowed procedures described in § 13.

3.4 *Status of signalling routes*

A signalling route can be in three states for signalling traffic having the concerned destination; these are available, restricted[4)], unavailable (see also Figure 6/Q.704).

3.4.1 *Signalling route unavailability*

A signalling route becomes unavailable when a transfer-prohibited message, indicating that signalling traffic towards a particular destination cannot be transferred via the signalling transfer point sending the concerned message, is received (see § 13).

3.4.2 *Signalling route availability*

A signalling route becomes available when a transfer-allowed message, indicating that signalling traffic towards a particular destination can be transferred via the signalling transfer point sending the concerned message, is received (see § 13).

---

4) National option.

3.4.3 *Signalling route restricted* [5]

A signalling route becomes restricted when a transfer-restricted message, indicating that the signalling traffic towards a particular destination is being transferred with some difficulty via the signalling transfer point sending the concerned message is received (see § 13).

3.5 *Procedures used in connection with route status changes*

In § 3.5 the procedures relating to each signalling management function, which in general are applied in connection with route status changes, are listed. See also Figures 6/Q.704 and 8/Q.704. Typical examples of the application of the procedures to particular network cases appear in Recommendation Q.705.

3.5.1 *Signalling route unavailable*

3.5.1.1 Signalling traffic management: the forced rerouting procedure (see § 7) is applied; it is used to transfer signalling traffic to the concerned destination from the link set, belonging to the unavailable route, to an alternative link set which terminates in another signalling transfer point. It includes actions to determine the alternative route.

3.5.1.2 Signalling route management: because of the unavailability of the signalling route, the network is reconfigured; in the case that a signalling transfer point can no longer route the concerned signalling traffic, it applies the procedures described in § 13.

3.5.2 *Signalling route available*

3.5.2.1 Signalling traffic management: the controlled rerouting procedure (see § 8) is applied; it is used to transfer signalling traffic to the concerned destination from a signalling link or link set belonging to an available route, to another link set which terminates in another signalling transfer point. It includes the determination of which traffic should be diverted and procedures for maintaining the correct message sequence.

3.5.2.2 Signalling route management: because of the restored availability of the signalling route, the network is reconfigured; in the case that a signalling transfer point can once again route the concerned signalling traffic, it applies the procedures described in § 13.

3.5.3 *Signalling route restricted* [5]

3.5.3.1 Signalling traffic management: the controlled rerouting procedure (see § 8) is applied; it is used to transfer signalling traffic to the concerned destination from the link set belonging to the restricted route, to an alternative link set if one is available to give more, if possible, efficient routing. It includes actions to determine the alternative route.

3.5.3.2 Signalling route management: because of restricted availability of the signalling route, the network routing is, if possible, reconfigured; procedures described in § 13 are used to advise adjacent signalling points.

3.6 *Status of signalling points*

A signalling point can be in two states; available or unavailable (see Figure 6/Q.704). However, implementation dependent congestion states may exist.

3.6.1 *Signalling point unavailability*

3.6.1.1 Unavailability of a signalling point itself: A signalling point becomes unavailable when all connected signalling links are unavailable.

---

[5] National option.

3.6.1.2 Unavailability of an adjacent signalling point: A signalling point considers that an adjacent signalling point becomes unavailable when:

- all signalling links connected to the adjacent signalling point are unavailable and
- the adjacent signalling point is inaccessible.

3.6.2 *Signalling point availability*

3.6.2.1 Availability of a signalling point itself: A signalling point becomes available when at least one signalling link connected to this signalling point becomes available.

3.6.2.2 Availability of an adjacent signalling point: A signalling point considers that an adjacent signalling point becomes available when:

- at least one signalling link connected to the adjacent signalling point becomes available and that signalling point has restarted, or
- the adjacent signalling point becomes accessible on the reception of a transfer allowed message or a transfer restricted[6] message (see § 13.4).

3.7 *Procedure used in connection with point status changes*

3.7.1 *Signalling point unavailable*

There is no specific procedure used when a signalling point becomes unavailable. The transfer prohibited procedure is used to update the status of the recovered routes in all nodes of the signalling network (see § 13.2).

3.7.2 *Signalling point available*

3.7.2.1 Signalling traffic management: the signalling point restart procedure (see § 9) is applied; it is used to restart the traffic between the signalling network and the signalling point which becomes available. This restart is based on the following criteria:

- avoid loss of messages
- limit the level 3 load due to the restart of a signalling point
- restart, as much as possible, simultaneously in both directions of the signalling relations.

3.7.2.2 Signalling link management: The first step of the signalling point restart procedure attempts to restore the signalling links of the point which becomes available; the signalling link restoration procedure is used (see § 12);

3.7.2.3 Signalling route management: The second step of the signalling point restart procedure consists of updating the signalling route states before carrying traffic to the point which becomes available and in all adjacent points; the transfer prohibited and transfer restricted[6] procedures are used (see § 13).

3.7.3 Signalling point congested: (implementation-dependent option, see § 11.2.6).

3.8 *Signalling network congestion*

3.8.1 *General*

In § 3.8, criteria for the determination of signalling link congestion status and signalling route set congestion status are specified. The procedures relating to each signalling network management function, which in general are applied in connection with congestion status changes, are listed.

---

[6] National option.

3.8.2 *Congestion status of signalling links*

3.8.2.1 When predetermined levels of MSU fill in the transmission or retransmission buffer are crossed, an indication is given to level 3 advising of congestion/congestion abatement. The location and setting of the congestion thresholds are considered to be implementation-dependent.

*Note* – The criterion for setting the congestion thresholds is based on: (1) the proportion of the total (transmit and retransmit) buffer capacity that is occupied, and/or (2) the total number of messages in the transmit and retransmit buffers. (The buffer capacity below the threshold should be sufficient to overcome load peaks due to signalling network management functions and the remaining buffer capacity should allow User Parts time to react to congestion indications before message discard occurs.) The monitoring may be performed in different ways depending on the relative sizes of the transmit and retransmit buffers. In the case of a relatively small retransmit buffer, monitoring of the transmit buffer may be sufficient. In the case of a relatively large retransmit buffer, both the transmit buffer and retransmit buffer occupancies may need to be monitored.

a) In the international signalling network, one congestion onset and one congestion abatement threshold are provided. The congestion abatement threshold should be placed lower than the congestion onset threshold in order to provide hysteresis during the process of recovering from congestion.

b) In national signalling networks, with multiple congestion thresholds, $N(1 \leqslant N \leqslant 3)$ separate thresholds are provided for detecting the onset of congestion. They are called congestion onset thresholds and are numbered $1, \ldots, N$, respectively. $N$ separate thresholds are provided for monitoring the abatement of congestion. They are called congestion abatement thresholds and are numbered $1, \ldots, N$, respectively.

3.8.2.2 In national signalling networks with multiple congestion thresholds $N$ separate thresholds are provided for determining whether, under congestion conditions, a message should be discarded or transmitted using the signalling link. They are called congestion discard thresholds and are numbered $1, \ldots, N$, respectively.

Congestion discard threshold $n(n = 1, \ldots, N)$ is placed higher than congestion onset threshold $n$ in order to minimize message loss under congestion conditions.

Congestion discard threshold $n(n = 1, \ldots, N - 1)$ should be placed at or lower than congestion onset threshold $n + 1$ in order to make congestion control effective.

When the current buffer occupancy does not exceed congestion discard threshold 1, the current signalling link discard status is assigned the zero value.

Each congestion abatement threshold should be placed lower than the corresponding congestion onset threshold in order to provide hysteresis during the process of recovering from congestion.

In national signalling networks with $N > 1$, the congestion abatement threshold $n(n = 2, \ldots, N)$ should be placed higher than the congestion onset threshold $n - 1$ so as to allow for a precise determination of signalling link congestion status.

Congestion abatement threshold 1 should be placed higher than the normally engineered buffer occupancy of a signalling link.

Under normal operation, when the signalling link is uncongested, the signalling link congestion status is assigned the zero value.

At the onset of congestion, when the buffer occupancy is increasing, the signalling link congestion status is determined by the highest congestion onset threshold exceeded by the buffer occupancy. That is, if congestion onset threshold $n(n = 1, \ldots, N)$ is the highest congestion onset threshold exceeded by the current buffer occupancy, the current signalling link congestion status is assigned the value $n$ (see Figure 8a/Q.704).

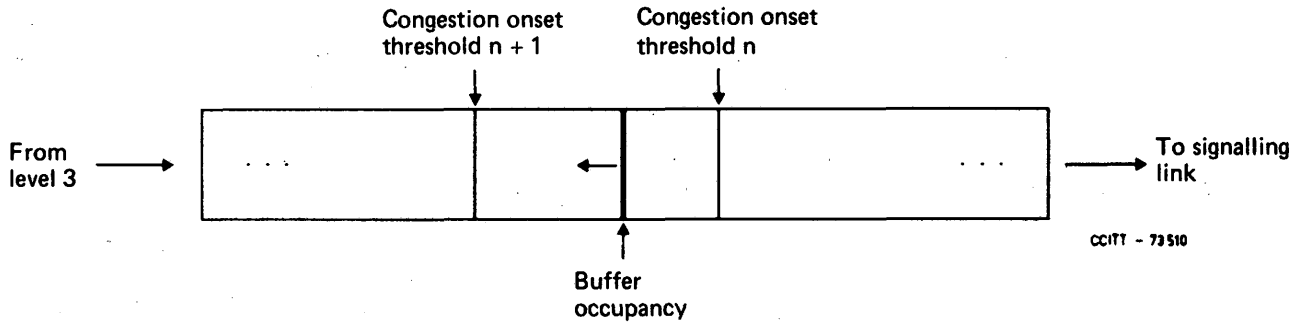



FIGURE 8a/Q.704

**Signalling link congestion status = n (congestion onset)**

At the abatement of congestion, when the buffer occupancy is decreasing, the signalling link congestion status is determined by the lowest congestion abatement threshold below which the buffer occupancy has dropped. That is, if congestion abatement threshold $n(n = 1, \ldots, N)$ is the lowest congestion abatement threshold below which the current buffer occupancy has dropped, the current signalling link congestion status is assigned the value $n - 1$ (see Figure 8b/Q.704).

The use of the signalling link congestion status is specified in § 2.3.5.2.

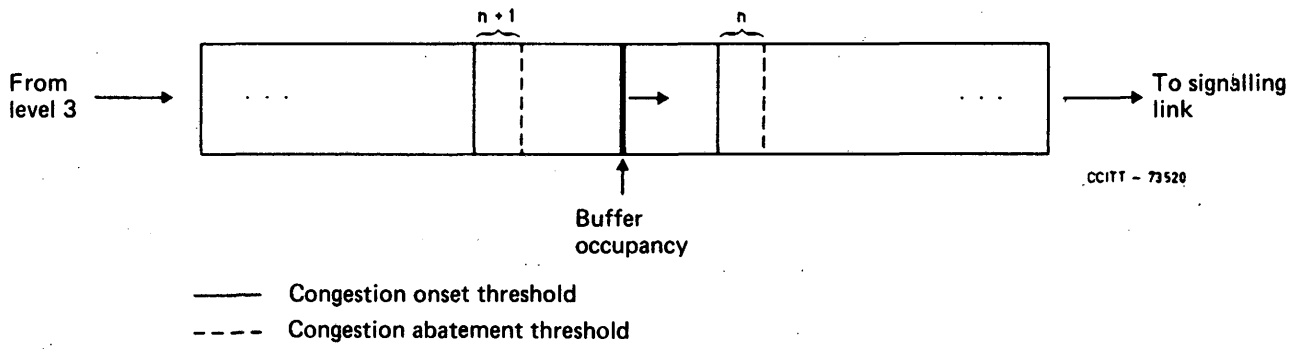



FIGURE 8b/Q.704

**Signalling link congestion status = n (congestion abatement)**

When the current buffer occupancy exceeds congestion discard threshold $n(n = 1, \ldots, N - 1)$, but does not exceed congestion discard threshold $n + 1$, the current signalling link discard status is assigned the value $n$ (see Figure 8c/Q.704).

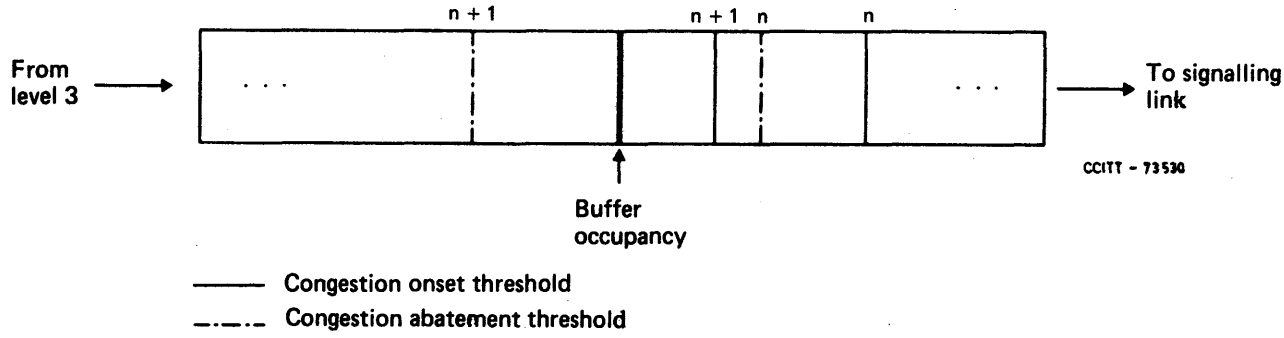



FIGURE 8c/Q.704

**Signalling link discard status = n**

When the current buffer occupancy exceeds congestion discard threshold *N*, the current signalling discard status is assigned the value *N*.

The use of the signalling link discard status is specified in § 2.3.5.2.

3.8.2.3 In national signalling networks using multiple signalling link congestion states without congestion priority, $S + 1 (1 \leqslant S \leqslant 3)$ levels of signalling link congestion status are accommodated in the signalling network, 0 being the lowest and *S* the highest.

The signalling link congestion status is determined by a timing mechanism after the buffer occupancy exceeds the congestion onset threshold, or drops below the congestion abatement threshold. Under normal operation, when the signalling link is uncongested, the signalling link congestion status is assigned the zero value.

At the onset of congestion, when the buffer occupancy exceeds the congestion onset threshold, the first signalling link congestion status is assigned a value *s*, predetermined in the signalling network.

If the signalling link congestion status is set to $s (s = 1, \ldots, S - 1)$ and the buffer occupancy continues to be above the congestion onset threshold during Tx, the signalling link congestion status is updated by the new value $s + 1$.

If the signalling link congestion status is set to $s (s = 1, \ldots, S)$ and the buffer occupancy continues to be below the abatement threshold during Ty, the signalling link congestion status is updated by the new value $s - 1$.

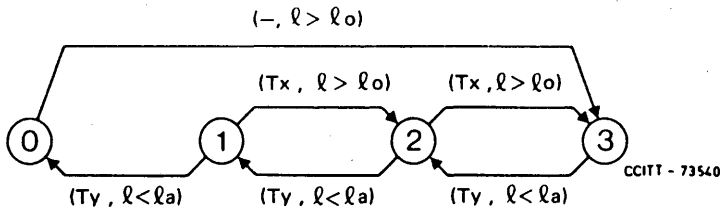
Otherwise, the current signalling link congestion status is maintained (see Figure 8d/Q.704).

The congestion abatement threshold should be placed lower than the congestion onset threshold.

3.8.3 *Procedures used in connection with link congestion status changes*

In § 3.8.3, the procedures relating to each signalling network management function, which in general are applied in connection with link congestion status changes, are listed.

Signalling route management: in the case when the congestion of a signalling link causes a signalling route set to become congested, the transfer-controlled procedure (see §§ 13.6 and 13.7) is used, if required, to notify originating signalling points that they should reduce the concerned signalling traffic towards the affected destination.




| | |
|---|---|
| 0~3 | Congestion status s |
| ℓ | Buffer occupancy |
| ℓo | Congestion onset threshold |
| ℓa | Congestion abatement threshold |
| ( , ) | Transition condition |
| Tx | Timing for updating s → s + 1 |
| Ty | Timing for updating s → s − 1 |
| – | Timing is zero |

FIGURE 8d/Q.704

**An example of signalling link congestion status**
**(using multiple signalling link congestion states without congestion priority)**

3.8.4 *Congestion status of signalling route sets*

At each originating signalling point, there is associated with each signalling route set a congestion status, which indicates the degree of congestion in the signalling route set.

a) In the international signalling network, two states are provided, congested and uncongested.

If a link in a signalling route towards a given destination becomes congested, the congestion status of the signalling route set towards the affected destination is changed to congested.

When a transfer controlled message relating to a given destination is received, the congestion status of the signalling route set towards the affected destination is indicated to the level 4 User Parts in accordance with the transfer-controlled procedure specified in § 13.6. The congestion status is not retained by level 3 at the receiving signalling point.

b) In national signalling networks with multiple congestion levels[7] corresponding to the $N + 1$ levels of signalling link congestion, there are $N + 1$ values of signalling route set congestion status, with 0 being the lowest and $N$ the highest.

Normally the congestion status of a signalling route set is assigned the zero value, indicating that the signalling route set is uncongested.

If a signalling link in the signalling route set to a given destination becomes congested, the congestion status of the signalling route set is assigned the value of the signalling link congestion status, if it is higher than the current signalling route set congestion status.

When a transfer-controlled message relating to a given destination is received, the congestion status of the signalling route set towards that destination is updated, in accordance with the transfer-controlled procedure as specified in § 13.7.

The congestion status of the signalling route set towards that destination may be decremented in accordance with the signalling-route-set-congestion-test procedure as specified in § 13.9.

[7] National option.

c) In national signalling networks using multiple congestion levels[8] without congestion priority, there are $S + 1$ values of signalling route set congestion states, with 0 being the lowest and $S$ the highest.

Normally the congestion status of a signalling route set is assigned the zero value, indicating that the signalling route set is uncongested.

If a local signalling link in the signalling route set to a given destination becomes congested, the congested status of the signalling route set is assigned the value of the signalling link congestion status, if it is larger than the current signalling route set congestion status.

When a transfer-controlled message relating to a given destination is received, the congestion status of the signalling route set towards that destination is updated in accordance with the transfer-controlled procedure as specified in § 13.8. The congestion status of the route set towards the congested destination is not retained by level 3 at the receiving signalling point.

3.8.5 *Procedures used in connection with route set congestion status changes*

In § 3.8.5, the procedures relating to each signalling network management function, which in general are applied in connection with route set congestion status changes, are listed.

3.8.5.1 Signalling traffic management: the signalling traffic flow control procedure (see § 11) is applied; it is used to regulate the input of signalling traffic from User Parts to the concerned signalling route set.

3.8.5.2 Signalling route management: as a national option, the signalling-route-set-congestion-test procedure (see § 13.9) is applied; it is used to update the congestion status of the concerned signalling route set until the congestion status is reduced to the zero value.

## 4 Signalling traffic management

### 4.1 *General*

4.1.1 The signalling traffic management function is used, as indicated in § 3, to divert signalling traffic from signalling links or routes, or to temporarily reduce it in quantity in the case of congestion.

4.1.2 The diversion of traffic in the cases of unavailability or availability or restriction[8] of signalling links and routes is typically made by means of the following basic procedures, included in the signalling traffic management function:

- signalling link unavailability (failure, deactivation, blocking or inhibiting): the changeover procedure (see § 5) is used to divert signalling traffic to one or more alternative links (if any);
- signalling link availability (restoration, activation, unblocking or uninhibiting): the changeback procedure (see § 6) is used to divert signalling traffic to the link made available;
- signalling route unavailability: the forced rerouting procedure (see § 7) is used to divert signalling traffic to an alternative route (if any);
- signalling route availability: the controlled rerouting procedure (see § 8) is used to divert signalling traffic to the route made available;
- signalling route restricted[8]: the controlled rerouting procedure (see § 8) is used to divert signalling traffic to an alternative route (if any);
- signalling point availability: the signalling point restart procedure (see § 9) is used to divert the signalling traffic to (or via) the point made available.

[8] National option.

Each procedure includes different elements of procedure, the application of one or more of which depends on the particular circumstances, as indicated in the relevant sections. Moreover, these procedures include a modification of the signalling routing, which is made in a systematic way, as described in §§ 4.2 to 4.7.

4.1.3 The signalling traffic flow control procedures are used in the case of congestion, in order to limit signalling traffic at its source. The procedures are specified in § 11.

## 4.2 *Normal routing situation*

4.2.1 Signalling traffic to be sent to a particular signalling point in the network, is normally routed to one or, in the case of load sharing between link sets in the international network, two link sets. A load sharing collection of one or more link sets is called a combined link set. Within a link set, a further routing may be performed in order to load share the traffic over the available signalling links (see § 2).

To cater for the situations when signalling links or routes become unavailable, alternative routing data are defined.

For each destination which may be reached from a signalling point, one or more alternative link sets (combined link sets) are allocated. An alternative combined link set may consist of one or more (or all) of the remaining available link sets, which may carry signalling traffic towards the concerned destination. The possible link set (combined link sets) appear in a certain priority order. The link set (combined link set) having the highest priority is used whenever it is available. It is defined that the normal link set (combined link set) for traffic to the concerned destination. The link set (combined link set) which is in use at a given time is called the current link set (combined link set). The current link set (combined link set) consists either of the normal link set (combined link set) or of an alternative link set (combined link set).

For each signalling link, the remaining signalling links in the link set are alternative links. The signalling links of a link set are arranged in a certain priority order. Under normal conditions the signalling link (or links) having the highest priority is used to carry the signalling traffic.

These signalling links are defined as normal signalling links, and each portion of load shared traffic has its own normal signalling link. Signalling links other than normal may be active signalling links (but not carrying any signalling traffic at the time) or inactive signalling links (see § 12).

4.2.2 Message routing (normal as well as alternative) is in principle independently defined at each signalling point. Thus, signalling traffic between two signalling points may be routed over different signalling links or paths in the two directions.

## 4.3 *Signalling link unavailability*

4.3.1 When a signalling link becomes unavailable (see § 3.2) signalling traffic carried by the link is transferred to one or more alternative links by means of a changeover procedure. The alternative link or links are determined in accordance with the following criteria.

4.3.2 In the case when there is one or more alternative signalling links available in the link set to which the unavailable link belongs, the signalling traffic is transferred within the link set to:

a) an active and unblocked signalling link, currently not carrying any traffic. If no such signalling link exists, the signalling traffic is transferred to

b) one or possibly more than one signalling link currently carrying traffic. In the case of transfer to one signalling link, the alternative signalling link is that having the highest priority of the signalling links in service.

4.3.3 In the case when there is no alternative signalling link within the link set to which the unavailable signalling link belongs, the signalling traffic is transferred to one or more alternative link sets (combined link sets) in accordance with the alternative routing defined for each destination. For a particular destination, the alternative link set (combined link set) is the link set (combined link set) in service having the highest priority.

Within a new link set, signalling traffic is distributed over the signalling links in accordance with the routing currently applicable for that link set; i.e., the transferred traffic is routed in the same way as the traffic already using the link set.

### 4.4 *Signalling link availability*

4.4.1 When a previously unavailable signalling link becomes available again (see § 3.2), signalling traffic may be transferred to the available signalling link by means of the changeback procedure. The traffic to be transferred is determined in accordance with the following criteria.

4.4.2 In the case when the link set, to which the available signalling link belongs, already carries signalling traffic on other signalling links in the link set, the traffic to be transferred is the traffic for which the available signalling link is the normal one.

The traffic is transferred from one or more signalling links, depending on the criteria applied when the signalling link became unavailable (see § 4.3.2).

4.4.3 In the case when the link set (combined link set) to which the available signalling links belongs, does not carry any signalling traffic [i.e., a link set (combined link set) has become available], the traffic to be transferred is the traffic for which the available link set (combined link set) has higher priority than the link set (combined link set) currently used.

The traffic is transferred from one or more link sets (combined link sets) and from one or more signalling links within each link set.

### 4.5 *Signalling route unavailability*

When a signalling route becomes unavailable (see § 3.4) signalling traffic currently carried by the unavailable route is transferred to an alternative route by means of forced re-routing procedure. The alternative route (i.e. the alternative link set or link sets) is determined in accordance with the alternative routing defined for the concerned destination (see § 4.3.3).

### 4.6 *Signalling route availability*

When a previously unavailable signalling route becomes available again (see § 3.4) signalling traffic may be transferred to the available route by means of a controlled rerouting procedure. This is applicable in the case when the available route (link set) has higher priority than the route (link set) currently used for traffic to the concerned destination (see § 4.4.3).

The transferred traffic is distributed over the links of the new link set in accordance with the routing currently applicable for that link set.

### 4.7 *Signalling route restriction*[9)]

When a signalling route becomes restricted (see § 3.4), signalling traffic carried by the restricted route is, if possible, transferred to an alternative route by means of the controlled rerouting procedure, if an equal priority alternative is available and not restricted. The alternative route is determined in accordance with alternate routing defined for the concerned destination (see § 4.3.3).

### 4.8 *Signalling point availability*

When a previously unavailable signalling point becomes available (see § 3.6), signalling traffic may be transferred to the available point by means of a signalling point restart procedure (see § 9).

---

9) National option.

## 5 Changeover

### 5.1 *General*

5.1.1 The objective of the changeover procedure is to ensure that signalling traffic carried by the unavailable signalling link is diverted to the alternative signalling link(s) as quickly as possible while avoiding message loss, duplication or mis-sequencing. For this purpose, in the normal case the changeover procedure includes buffer updating and retrieval, which are performed before reopening the alternative signalling link(s) to the diverted traffic. Buffer updating consists of identifying all those messages in the retransmission buffer of the unavailable signalling link which have not been received by the far end. This is done by means of a hand-shake procedure, based on changeover messages, performed between the two ends of the unavailable signalling link. Retrieval consists of transferring the concerned messages to the transmission buffer(s) of the alternative link(s).

5.1.2 Changeover includes the procedures to be used in the case of unavailability (due to failure, blocking or inhibiting) of a signalling link, in order to divert the traffic pertaining to that signalling link to one or more alternative signalling links.

These signalling links can be carrying their own signalling traffic and this is not interrupted by the changeover procedure.

The different network configurations to which the changeover procedure may be applied are described in § 5.2.

The criteria for initiation of changeover, as well as the basic actions to be performed, are described in § 5.3.

Procedures necessary to cater for equipment failure or other abnormal conditions are also provided.

### 5.2 *Network configurations for changeover*

5.2.1 Signalling traffic diverted from an unavailable signalling link is routed by the concerned signalling point according to the rules specified in § 4. In summary, two alternative situations may arise (either for the whole diverted traffic or for traffic relating to each particular destination):

i) traffic is diverted to one or more signalling links of the same link set, or

ii) traffic is diverted to one or more different link sets.

5.2.2 As a result of these arrangements, and of the message routing function described in § 2, three different relationships between the new signalling link and the unavailable one can be identified, for each particular traffic flow. These three basic cases may be summarized as follows:

a) the new signalling link is parallel to the unavailable one (see Figure 9/Q.704);

b) the new signalling link belongs to a signalling route other than that to which the unavailable signalling link belongs, but this signalling route still passes through the signalling point at the far end of the unavailable signalling link (see Figure 10/Q.704);

c) the new signalling link belongs to a signalling route other than that to which the unavailable signalling link belongs, and this signalling route does not pass through the signalling point acting as signalling transfer point, at the far end of the unavailable signalling link (see Figure 11/Q.704).

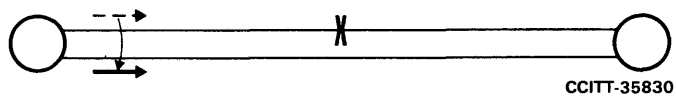



FIGURE 9/Q.704

**Example of changeover to a parallel link**

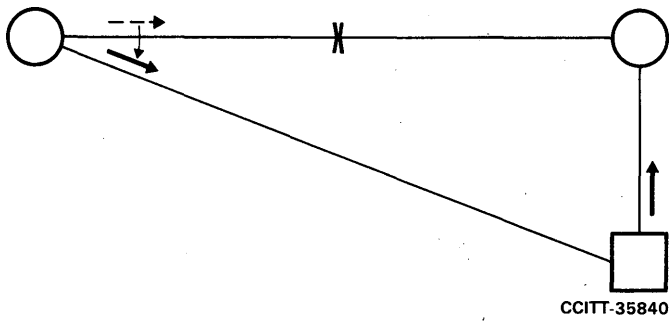



FIGURE 10/Q.704

**Example of changeover to a signalling route passing through the remote signalling point**

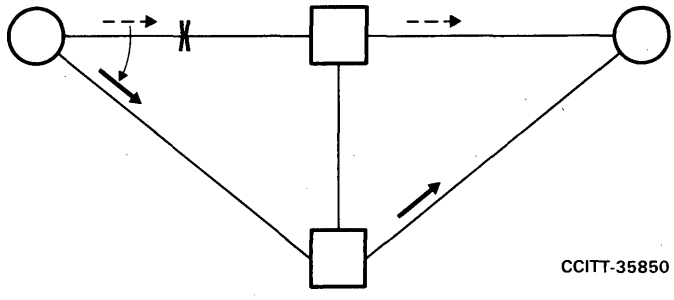



FIGURE 11/Q.704

**Example of changeover to a signalling route not passing through the remote signalling point**

Only in the case of c) does a possibility of message mis-sequencing exist: therefore its use should take into account the overall service dependability requirements described in Recommendation Q.706.

5.3 *Changeover initiation and actions*

5.3.1 Changeover is initiated at a signalling point when a signalling link is recognized as unavailable according to the criteria listed in § 3.2.2.

The following actions are then performed:

a) transmission and acceptance of message signal units on the concerned signalling link is terminated;

b) transmission of link status signal units or fill in signal units, as described in Recommendation Q.703, § 5.3, takes place;

c) the alternative signalling link(s) are determined according to the rules specified in § 4;

d) a procedure to update the content of the retransmission buffer of the unavailable signalling link is performed as specified in § 5.4 below;

e) signalling traffic is diverted to the alternative signalling link(s) as specified in § 5.5 below.

In addition, if traffic toward a given destination is diverted to an alternative signalling link terminating in a signalling transfer point not currently used to carry traffic toward that destination, a transfer-prohibited procedure is performed as specified in § 13.2.

5.3.2 In the case when there is no traffic to transfer from the unavailable signalling link action, only item b) of § 5.3.1 is required.

5.3.3 If no alternative signalling link exists for signalling traffic towards one or more destinations, the concerned destination(s) are declared inaccessible and the following actions apply:

i) the routing of the concerned signalling traffic is blocked and the concerned messages already stored in the transmission and retransmission buffers of the unavailable signalling link, as well as those received subsequently, are discarded [10];

ii) a command is sent to the User Part(s) (if any) in order to stop generating the concerned signalling traffic;

iii) the transfer-prohibited procedure is performed, as specified in § 13.2;

iv) the appropriate signalling link management procedures are performed, as specified in § 12.

5.3.4 In some cases of failures or in some network configurations, the normal buffer updating and retrieval procedures described in §§ 5.4 and 5.5 cannot be accomplished. In such cases, the emergency changeover procedures described in § 5.6 apply.

Other procedures to cover possible abnormal cases appear in § 5.7.

## 5.4 *Buffer updating procedure*

5.4.1 When a decision to changeover is made, a changeover order is sent to the remote signalling point. In the case that the changeover was initiated by the reception of a changeover order (see § 5.2) a changeover acknowledgement is sent instead.

A changeover order is always acknowledged by a changeover acknowledgement, even when changeover has already been initiated in accordance with another criterion.

No priority is given to the changeover order or changeover acknowledgement in relation to the normal traffic of the signalling link on which the message is sent.

5.4.2 The changeover order and changeover acknowledgement are signalling network management messages and contain the following information:

- the label, indicating the destination and originating signalling points and the identity of the unavailable signalling link;
- the changeover-order (or changeover-acknowledgement) signal; and
- the forward sequence number of the last message signal unit accepted from the unavailable signalling link.

Formats and codes of the changeover order and the changeover acknowledgement appear in § 15.

5.4.3 Upon reception of a changeover order or changeover acknowledgement, the retransmission buffer of the unavailable signalling link is updated (except as noted in § 5.6), according to the information contained in the message. The message signal units successive to that indicated by the message are those which have to be retransmitted on the alternative signalling link(s), according to the retrieval and diversion procedure.

## 5.5 *Retrieval and diversion of traffic*

When the procedure to update the retransmission buffer content is completed, the following actions are performed:

- the routing of the signalling traffic to be diverted is changed;
- the signal traffic already stored in the transmission buffers and retransmission buffer of the unavailable signalling link is sent directly towards the new signalling link(s), according to the modified routing.

The diverted signalling traffic will be sent towards the new signalling link(s) in such a way that the correct message sequence is maintained. The diverted traffic has no priority in relation to normal traffic already conveyed on the signalling link(s).

---

[10] The adequacy of this procedure to meet the acceptable dependability objective in terms of loss of messages requires further study.

5.6 *Emergency changeover procedures*

5.6.1 Due to the failure in a signalling terminal it may be impossible for the corresponding end of the faulty signalling link to determine the forward sequence number of the last message signal unit accepted over the unavailable link. In this case, the concerned end accomplishes, if possible, the buffer updating procedures described in § 5.4 but it makes use of an emergency changeover order or an emergency changeover acknowledgement instead of the corresponding normal message; these emergency messages, the format of which appears in § 15, do not contain the forward sequence number of the last accepted message signal unit. Furthermore, the signalling link is taken out of service, i.e. the concerned end initiates, if possible, the sending of *out-of-service* link status signal units on the unavailable link (see Recommendation Q.703, § 5.3).

When the other end of the unavailable signalling link receives the emergency changeover order or acknowledgement, it accomplishes the changeover procedures described in §§ 5.4 and 5.5, the only difference being that it does not perform either buffer updating or retrieval. Instead, it directly starts sending the signalling traffic not yet transmitted on the unavailable link on the alternative signalling link(s).

The use of normal or emergency changeover messages depends on the local conditions of the sending signalling point only, in particular:

- an emergency changeover order is acknowledged by a changeover acknowledgement if the local conditions are normal; and
- a changeover order is acknowledged by an emergency changeover acknowledgement if there are local fault conditions.

5.6.2 Time-controlled changeover is initiated when the exchange of changeover messages is not possible or not desirable, i.e., if any (or several) of the following cases apply:

i) No signalling path exists between the two ends of the unavailable link, so that the exchange of changeover messages is impossible.

ii) Processor outage indication is received on a link. In this case, if the remote processor outage condition is only transitory, sending of a changeover order could result in failure of the link.

iii) A signalling link currently carrying traffic has been marked (locally or remotely) inhibited. In this case, time controlled changeover is used to divert traffic for the inhibited link without causing the link to fail.

When the concerned signalling point decides to initiate changeover in such circumstances, after the expiry of a time T1 (see § 16.8), it starts signalling traffic not yet transmitted on the unavailable signalling link on the alternative link(s); the purpose of withholding traffic for the time T1 (see § 16.8) is to reduce the probability of message mis-sequencing.

An example of such a case appears in Recommendation Q.705, Annex A.

In the abnormal case when the concerned signalling point is not aware of the situation, it will start the normal changeover procedure and send a changeover order; in this case it will receive no changeover message in response and the procedure will be completed as indicated in § 5.7.2. Possible reception of a transfer-prohibited message (sent by an involved signalling transfer point on reception of the changeover order, see § 13.2) will not affect changeover procedures.

5.6.3 Due to failures, it may be impossible for a signalling point to perform retrieval even if it has received the retrieval information from the far end of the unavailable signalling link. In this case, it starts sending new traffic on reception of the changeover message (or on time-out expiry, see §§ 5.6.2 and 5.7.2); no further actions in addition to the other normal changeover procedures are performed.

5.7 *Procedures in abnormal conditions*

5.7.1 The procedures described in this section allow the completion of the changeover procedures in abnormal cases other than those described in § 5.6.

5.7.2 If no changeover message in response to a changeover order is received within a timer T2 (see § 16.8), new traffic is started on the alternative signalling link(s).

5.7.3 If a changeover order or acknowledgement containing an unreasonable value of the forward sequence number is received, no buffer updating or retrieval is performed, and new traffic is started on the alternative signalling link(s).

5.7.4 If a changeover acknowledgement is received without having previously sent a changeover order, no action is taken.

5.7.5 If a changeover order is received relating to a particular signalling link after the completion of changeover from that signalling link, an emergency changeover acknowledgement is sent in response, without any further action.

## 6 Changeback

### 6.1 *General*

6.1.1 The objective of the changeback procedure is to ensure that signalling traffic is diverted from the alternative signalling link(s) to the signalling link made available as quickly as possible, while avoiding message loss, duplication or mis-sequencing. For this purpose (in the normal case), changeback includes a procedure to control the message sequence.

6.1.2 Changeback includes the basic procedures to be used to perform the opposite action to changeover, i.e. to divert traffic from the alternative signalling link(s) to a signalling link which has become available (i.e., it was uninhibited, restored or unblocked). The characteristics of the alternative signalling link(s) from which changeback can be made are described in § 5.2. In all the cases mentioned in § 5.2 the alternative signalling links can be carrying their own signalling traffic and this is not interrupted by the changeback procedures.

Procedures necessary to cater for particular network configuration or other abnormal conditions are also provided.

*Note* – The term "alternative signalling link(s)" refers to signalling link(s) terminating in the signalling point at which a changeback is initiated (see also § 4).

### 6.2 *Changeback initiation and actions*

6.2.1 Changeback is initiated at a signalling point when a signalling link is restored, unblocked or uninhibited, and therefore it becomes once again available, according to the criteria listed in §§ 3.2.3 and 3.2.7. The following actions are then performed:

a) the alternative signalling link(s) are determined, to which traffic normally carried by the signalling link made available was previously diverted (e.g., on occurrence of a changeover);

b) signalling traffic is diverted (if appropriate, according to the criteria specified in § 4) to the concerned signalling link by means of the sequence control procedure specified in § 6.3; traffic diversion can be performed at the discretion of the signalling point initiating changeback, as follows:

   i) individually for each traffic flow (i.e., on destination basis);

   ii) individually for each alternative signalling link (i.e., for all the destinations previously diverted on that alternative signalling link);

   iii) at the same time for a number of, or for all the alternative signalling links.

On occurrence of changeback, it may happen that traffic towards a given destination is no longer routed via a given adjacent signalling transfer point, towards which a transfer-prohibited procedure was previously performed on occurrence of changeover (see § 5.3.1); in this case a transfer-allowed procedure is performed, as specified in § 13.3.

In addition, if traffic towards a given destination is diverted to an alternative signalling link terminating in a signalling transfer point not currently used to carry traffic toward that destination, a transfer-prohibited procedure is performed as specified in § 13.2.

6.2.2 In the case when there is no traffic to transfer to the signalling link made available, none of the previous actions are performed.

6.2.3 In the case that the signalling link made available can be used to carry signalling traffic toward a destination which was previously declared inaccessible, the following actions apply:

i) the routing of the concerned signalling traffic is unblocked and transmission of the concerned messages (if any) is immediately started on the link made available;

ii) a command is sent to the User Part(s) (if any) in order to restart generating the concerned signalling traffic;

iii) the transfer-allowed procedure is performed, as specified in § 13.3. However, in national networks, when the recovered link is not on the normal route for that destination, the transfer-restricted[11] procedure may be performed as specified in § 13.5.

6.2.4 In the case that the signalling link made available is used to carry signalling traffic towards a destination which was previously declared restricted, the following actions apply:

i) the concerned signalling traffic is rediverted and transmission of the concerned messages (if any) is immediately started on the link made available;

ii) when the recovered link is on the normal route for that destination, the status of the route is changed to available; otherwise, the status of the route remains unchanged.

6.2.5 If the signalling point at the far end of the link made available currently is inaccessible, from the signalling point initiating changeback (see § 9 on Signalling Point Restart), the sequence control procedure specified in § 6.3 (which requires communication between the two concerned signalling points) does not apply; instead, the time-controlled diversion specified in § 6.4 is performed. This is made also when the concerned signalling points are accessible, but there is no signalling route to it using the same outgoing signalling link(s) (or one of the same signalling links) from which traffic will be diverted.

6.3 *Sequence control procedure*

6.3.1 When a decision is made at a given signalling point to divert a given traffic flow (towards one or more destinations) from an alternative signalling link to the signalling link made available, the following actions are performed if possible (see § 6.4):

i) transmission of the concerned traffic on the alternative signalling link is stopped; such traffic is stored in a *changeback buffer*;

ii) a changeback declaration is sent to the remote signalling point of the signalling link made available via the concerned alternative signalling link; this message indicates that no more message signal units relating to the traffic being diverted to the link made available will be sent on the alternative signalling link.

6.3.2 The concerned signalling point will restart diverted traffic over the signalling link made available when it receives a changeback acknowledgement from the far signalling point of the link made available; this message indicates that all signal messages relating to the concerned traffic flow and routed to the remote signalling point via the alternative signalling link have been received. The remote signalling point will send the changeback acknowledgement to the signalling point initiating changeback in response to the changeback declaration; any available signalling route between the two signalling points can be used to carry the changeback acknowledgement.

6.3.3 The changeback declaration and changeback acknowledgement are signalling network management messages and contain:

– the label, indicating the destination and originating signalling points, and the identity of the signalling link to which traffic will be diverted;

– the changeback-declaration (or changeback-acknowledgement) signal, and

– the changeback code.

Formats and codes of the changeback declaration and changeback acknowledgement appear in § 15.

[11] National option.

6.3.4 A particular configuration of the changeback code is autonomously assigned to the changeback declaration by the signalling point initiating changeback; the same configuration is included in the changeback acknowledgement by the acknowledging signalling point. This allows discrimination between different changeback declarations and acknowledgements when more than one sequence control procedures are initiated in parallel, as follows.

6.3.5 In the case that a signalling point intends to initiate changeback in parallel from more than one alternative signalling link, a sequence control procedure is accomplished for each involved signalling link, and a changeback declaration is sent on each of them; each changeback declaration is assigned a different configuration of the changeback code. Stopped traffic is stored in one or more changeback buffers (in the latter case, a changeback buffer is provided for each alternative signalling link). When the changeback acknowledgement relating to that alternative signalling link is received, traffic being diverted from a given alternative signalling link can be restarted on the signalling link made available, starting with the content of the changeback buffer; discrimination between the different changeback acknowledgements is made by the changeback code configuration, which is the same as that sent in the changeback declaration.

This procedure allows either reopening the recovered signalling link to traffic in a selective manner (provided that different changeback buffers are used) as soon as each changeback acknowledgement is received, or only when all the changeback acknowledgements have been received.

## 6.4 *Time-controlled diversion procedure*

6.4.1 The time-controlled diversion procedure is used at the end of the signalling point restart procedure (see § 9) when an adjacent signalling point becomes available, as well as for the reasons given in § 6.2.5. An example of such a use appears in Figure 12/Q.704.

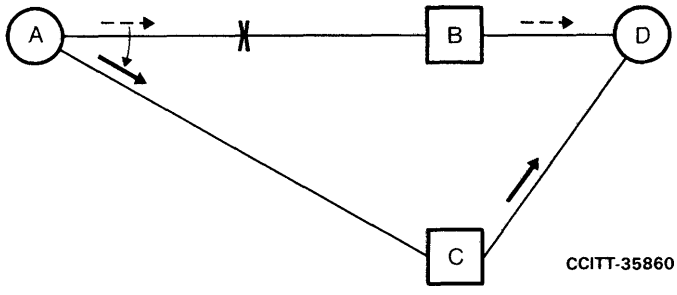



FIGURE 12/Q.704
**Example of time-controlled diversion procedure**

In this example, on failure of signalling link AB, traffic towards the destination D was directed to signalling link AC. When AB becomes available, the point A considers itself as the neighbour of a point which restarts and applies the signalling point restart procedure (see § 9).

6.4.2 When changeback is initiated after the signalling point restart procedure, the adjacent signalling point of the point which is restarting stops traffic to be directed from the alternative signalling link(s) for a time T3, after which it starts traffic on the signalling link(s) made available. The time delay minimizes the probability of out-of-sequence delivery to the destination point(s).

## 6.5 *Procedures in abnormal conditions*

6.5.1 If a changeback acknowledgement is received by a signalling point which has not previously sent a changeback declaration, no action is taken.

6.5.2 If a changeback declaration is received after the completion of the changeback procedure, a changeback acknowledgement is sent in response, without taking any further action. This corresponds to the normal action described in § 6.3.2 above.

6.5.3 If no changeback acknowledgement is received in response to a changeback declaration within a time T4 (see § 16.8), the changeback declaration is repeated and a new timer T5 (see § 16.8), is started. If no changeback acknowledgement is received before the expiry of T5, the maintenance functions are alerted and traffic on the link made available is started. The changeback code contained in the changeback acknowledgement message makes it possible to determine, in the case of parallel changebacks from more than one reserve path, which changeback declaration is unacknowledged and has therefore to be repeated.

## 7 Forced rerouting

### 7.1 *General*

7.1.1 The objective of the forced rerouting procedure is to restore, as quickly as possible, the signalling capability between two signalling points towards a particular destination, in such a way as to minimize the consequences of a failure. However, since the unavailability of a signalling route is, in general, caused by the fact that the concerned destination has become inaccessible to a signalling transfer point, a probability of message loss exists (see § 5.3.3). Therefore, the structure of the signalling network should be such as to reduce the probability of signalling route unavailability to limits compatible with the overall dependability requirements (see Recommendation Q.706).

7.1.2 Forced rerouting is the basic procedure to be used in the case where a signalling route towards a given destination becomes unavailable (due to, for example, remote failures in the signalling network) to divert signalling traffic towards that destination to an alternative signalling route outgoing from the concerned signalling point. Signalling links pertaining to the alternative signalling route can be carrying their own signalling traffic (relating to different signalling routes), and this is not interrupted by the forced rerouting procedure.

### 7.2 *Forced rerouting initiation and actions*

7.2.1 Forced rerouting is initiated at a signalling point when a transfer-prohibited message, indicating a signalling route unavailability is received.

The following actions are then performed:

a) transmission of signalling traffic towards the concerned destination on the link set(s) pertaining to the unavailable route is immediately stopped; such traffic is stored in a *forced rerouting buffer*;

b) the alternative route is determined according to the rules specified in § 4;

c) as soon as action b) is completed, the concerned signalling traffic is restarted on a link set pertaining to the alternative route, starting with the content of the forced rerouting buffer;

d) if appropriate, a transfer-prohibited procedure is performed (see § 13.2.2).

7.2.2 In the case when there is no signalling traffic to be diverted from the unavailable route, action b) and d) apply.

7.2.3 If no alternative route exists for signalling traffic towards the concerned destination, that destination is declared inaccessible, and the actions specified in § 5.3.3 apply.

## 8 Controlled rerouting

### 8.1 *General*

8.1.1 The objective of the controlled rerouting procedure is to restore the optimal signalling routing and to minimize mis-sequencing of messages. Therefore, controlled rerouting includes a time-controlled traffic diversion procedure, which is the same as that used in some cases of changeback (see § 6.4).

8.1.2 Controlled rerouting is the basic procedure to be used in the following two cases:

a) when a signalling route towards a given destination becomes available (due to, for example, recovery of previous remote failures in the signalling network), to divert back signalling traffic towards that destination from the alternative to the normal signalling route outgoing from the concerned signalling point;

b) when a transfer-restricted [12] message is received, after signalling traffic management has decided that alternative routing is appropriate (e.g., because it would be more efficient than routing via the link set over which the transfer-restricted message was received).

Signalling links pertaining to the alternative signalling route can be carrying their own signalling traffic (relating to different routes) and this is not interrupted by the controlled rerouting procedure.

8.2 *Controlled rerouting initiation and actions*

8.2.1 Controlled rerouting is initiated at a signalling point when a transfer-allowed message, indicating that the signalling route has become available, is received; also when a transfer-restricted [12] message is received.

The following actions are then performed:

a) transmission of signalling traffic towards the concerned destination on the link set belonging to the alternative route or the route over which the transfer-restricted [12] message was received is stopped; such traffic is stored in a "controlled rerouting buffer"; a timer T6 (see § 16.8), is started;

b) if the signalling point serves as a signalling transfer point, a transfer-prohibited procedure is performed for the route made available (or the alternative route in the case of reception of a transfer-restricted [12] message, if the alternative route was not previously used), and a transfer-allowed procedure for the alternative one (or on the restricted route in the case of the reception of a transfer-restricted [12] message) (see §§ 13.2.2 and 13.3.2, respectively);

c) at the expiry of T6, the concerned signalling traffic is restarted on an outgoing link set pertaining to the signalling route made available, or the alternative route in the case of reception of the transfer-restricted [12] message, starting with the content of the controlled rerouting buffer; the aim of the time delay is to minimize the probability of out-of-sequence delivery to the destination point(s).

8.2.2 In the case when there is no signalling traffic to be diverted from the route made available, only action b) applies.

8.2.3 If the destination was inaccessible or restricted [12], when the route is made available, then the destination is declared accessible and actions specified in §§ 6.2.3 and 6.2.4 apply (if appropriate).

## 9 Signalling point restart

This procedure uses the Traffic Restart Allowed message (TRA) which contains:

- the label indicating the originating signalling point and adjacent destination signalling point;
- the traffic restart allowed signal.

The format and coding of this message appear in § 15.

9.1 *Actions in a signalling point (having the transfer function) which restarts*

A signalling point restarts when it becomes available (see § 3.6.2.1). A signalling point which restarts starts a timer T18 and starts activating all its signalling links (see § 12).

When the first signalling link of a signalling link set is available, message traffic terminating at the far end of the linkset is immediately restarted (see also § 9.5).

The restarting signalling point takes into account any transfer prohibited, transfer restricted [12] (see § 13) and traffic restart allowed messages received.

When all signalling links are available T18 is stopped.

---

[12] National option.

When T18 is stopped or expires, the following actions are taken:

- the signalling point starts a timer T19 during which it expects to receive additional transfer prohibited, transfer restricted[13] (see § 13) and traffic restart allowed messages;
- when all traffic restart allowed messages are received T19 is stopped.

When T19 is stopped or expires, the signalling point starts a timer T20 during which:

- it broadcasts eventually transfer prohibited and transfer restricted[13] messages (see § 13), taking into account signalling links which are not available and any transfer prohibited and transfer restricted[13] messages eventually received;
- when all these operations are completed, timer T20 is stopped.

When T20 is stopped or expires, the signalling point broadcasts traffic restart allowed messages to all adjacent signalling points and restarts the remaining traffic.

### 9.2 *Actions in a restarting signalling point (having no transfer function)*

An SP which restarts starts a timer T21 and starts activating all its signalling links (see § 12).

When the first signalling link of a signalling linkset is available, message traffic terminating at the far end of the linkset is immediately restarted (see also § 9.5).

The restarting signalling point takes into account transfer prohibited and transfer restricted messages[13] (see § 13). If a traffic restart allowed message is received T21 is stopped. When T21 is stopped or expires, the signalling point restarts the remaining traffic.

### 9.3 *Actions in a signalling point X adjacent to a restarting signalling point Y*

Signalling point X knows that signalling point Y is restarting when signalling point Y becomes accessible (see § 3.6.2.2). There are three cases to consider:

i) Signalling points X and Y have the transfer function

a) When signalling point Y becomes accessible because a direct linkset becomes available, signalling point X takes the following action:

- starts a timer T21
- immediately restarts traffic terminating in signalling point Y (see also § 9.5)
- sends any eventual transfer prohibited and transfer restricted[13] messages to signalling point Y (see § 13)
- sends a traffic restart allowed message to signalling point Y
- takes into account the eventual transfer prohibited and transfer restricted[13] messages received from SP Y (see § 13).

When a traffic restart allowed message is received from signalling point Y, timer T21 is stopped. When T21 is stopped or expires, signalling point X restarts any remaining traffic to Y, and broadcasts transfer allowed messages concerning Y, and all SPs made accessible via Y.

b) When signalling point Y becomes accessible on reception of a transfer allowed or transfer restricted[13] message (see § 13), signalling point X sends to signalling point Y any required transfer prohibited and transfer restricted messages[13] on the available route.

ii) Signalling point X has a transfer function and signalling point Y has not

a) When signalling point Y becomes accessible because a direct signalling linkset becomes available, signalling point X takes the following actions:

- immediately restarts traffic terminating in signalling point Y (see also § 9.5)
- eventually sends to signalling point Y any transfer prohibited and transfer restricted[13] messages (see § 13)
- broadcasts transfer allowed messages concerning signalling point Y and sends a traffic restart allowed message to it.

---

[13] National option.

b) When signalling point Y becomes accessible on reception of a transfer allowed or transfer restricted[14] message, signalling point X sends to signalling point Y any required transfer prohibited and transfer restricted[14] messages on the available route.

iii) Signalling point X does not have the transfer function and signalling point Y does or does not have the transfer function.

Signalling point X takes the following action:

- immediately restarts traffic terminating at signalling point Y (see also § 9.5)
- starts a timer T21
- takes into account any eventual transfer prohibited and transfer restricted[14] message received.

On the receipt of a traffic restart allowed message, timer T21 is stopped. When T21 is stopped or expires, signalling point X restarts any remaining traffic.

### 9.4 *Actions in signalling point X on receipt of unexpected TRA message*

If X has no STP function, no further action is taken.

If X has the STP function, then X sends to the adjacent point Y, from which the TRA message was received, the appropriate TFP and TFR messages. X then operates normally.

### 9.5 *General rules*

When a signalling point restarts, it considers, at the beginning of the point restart procedure, all signalling routes to be allowed. A signalling route set test message received in a restarting signalling point (during the point restart procedure) is ignored.

Signalling route set test messages received in a signalling point adjacent to a restarting signalling point (before T21 expires) are handled, but the replies consider that all signalling routes using the restarting point are prohibited. When T21 is stopped or expires these signalling routes are allowed unless a transfer prohibited or transfer restricted[14] message has been received from the restarting signalling point during T21.

The procedure includes the general rule that late events [e.g., restoration of a link after T18 expires, transfer prohibited or transfer restricted[14] messages received after T19 expires, etc.] are treated outside the restart procedure.

All messages concerning another destination received in a restarting signalling point are treated normally during the point restart procedure. All messages concerning a local MTP user received in a restarting signalling point (Service Indicator != 0000) are treated normally. All messages received with Service Indicator = 0000 in a restarting signalling point, for the signalling point itself, are treated as described in the signalling point restart procedure; those messages not described elsewhere in the procedure are discarded and no action is taken (message groups CHM, ECM, FCM, RSM, MIM and DLM).

## 10 Management inhibiting

### 10.1 *General*

Signalling link management inhibiting is requested by management when it becomes necessary e.g., for maintenance or testing purposes (for example, if the link experiences too many changeovers and changebacks in a short time, or there is a significant link error rate), to make or keep a signalling link unavailable to User Part-generated signalling traffic. Management inhibiting is a signalling traffic management action, and does not cause any link status changes at level 2. A signalling link is marked "inhibited" under the management inhibiting procedure. In particular, a signalling link that was active and in service prior to being inhibited will remain so, and will thus be able to transmit maintenance and test messages.

Inhibiting of a signalling link may be requested by management functions at either end of the link. The request is granted, provided that the inhibiting action does not cause any previously accessible destinations to become inaccessible at either end of the signalling link. The request may also be refused under certain circumstances such as congestion.

---

[14] National option.

A signalling link normally remains inhibited until uninhibiting is invoked in the signalling point at which inhibiting was initiated. Uninhibiting is initiated either at the request of a management function or by routing functions at either end of the signalling link when it is found that a destination has become inaccessible for signalling traffic and the link sets associated with routes to that destination contain inhibited links. Unless unavailable for other reasons, uninhibiting causes the signalling link to enter the available state and changeback to be initiated.

Periodic tests are made on the inhibit status of inhibited links. Such periodic tests should not add significantly to the traffic load on the signalling network, and remove the need for a signalling point to perform inhibit tests at signalling point restart.

If a test on the inhibit status of a link reveals discrepancies between the signalling points at each end of the link, the link is either uninhibited or force uninhibited as appropriate, to align the inhibit status at each end of the link.

### 10.2 *Inhibiting initiation and actions*

When at signalling point "X" a request is received from a management function to inhibit a signalling link to signalling point "Y", the following actions take place:

a) A check is performed at signalling point "X" to determine whether, in the case of an available link, inhibiting will result in a destination becoming inaccessible, or in the case of an unavailable link, signalling point "Y" is inaccessible. If either is the case, management is informed that the inhibiting request is denied.

b) If inhibiting is permitted, signalling point "X" sends an inhibit message to signalling point "Y" indicating that it wishes to inhibit the signalling link identified in the message.

c) Signalling point "Y", on receiving the inhibit message from "X", checks whether, in the case of an available link, inhibiting will result in a destination becoming inaccessible and, if so, an inhibit denied message is returned to signalling point "X". The latter then informs the management function which requested inhibiting that the request cannot be granted.

d) If the signalling point "Y" finds that inhibiting of the concerned link is permissible, it sends an inhibit acknowledgement to signalling point "X" and marks the link remotely inhibited.

   If the link concerned is currently carrying traffic, signalling point "Y" sends the inhibit acknowledgement via that link and diverts subsequent traffic for it, using the time controlled changeover procedure. "Y" then starts inhibit test timer T23.

e) On receiving an inhibit acknowledgement message, signalling point "X" marks the link locally inhibited and informs management that the link is inhibited.

   If the link concerned is currently carrying traffic, signalling point "X" diverts subsequent traffic for that link, using the time-controlled changeover procedure. "X" then starts inhibit test timer T22.

f) When changeover has been completed, the link while inhibited, will be unavailable for the transfer of user-generated traffic but still permits the exchange of test messages.

g) If, for any reason, the inhibit acknowledgement message is not received, a timer T14 expires and the procedure is restarted including inspection of the status of the destination of the inhibit message. If the destination is not available, management is informed.

At most two consecutive automatic attempts may be made to inhibit a particular signalling link.

A signalling point may not transmit an inhibit message for a particular signalling link if it has already transmitted an uninhibit message for that link, and neither an acknowledgement for that uninhibit message has been received nor has the uninhibit procedure finally timed out.

### 10.3 *Uninhibiting initiation and actions*

Signalling link uninhibiting is initiated at the signalling point which originally caused the link to be inhibited, upon receipt of an uninhibit or forced uninhibit request.

In a given signalling point, an uninhibit request may be initiated for a locally inhibited link by the management or signalling routing control function, while a forced uninhibit request may be initiated for a remotely inhibited link by the signalling routing control function only.

Signalling routing control will initiate signalling link uninhibit if an inhibited link is found to be a member of a link set in a route to a destination which has become inaccessible.

If such signalling routing control uninhibiting were unsuccessful because of a failed or blocked inhibited link, and if that link later recovers or becomes unblocked with the destination still unavailable, uninhibiting is re-attempted.

A signalling point may not transmit an uninhibit message for a particular signalling link if it has already transmitted an inhibit message for that link, and neither an acknowledgement for that inhibit message has been received nor has the inhibit procedure finally timed out.

### 10.3.1 *Management-initiated uninhibiting*

Upon receipt of an uninhibiting request from the management function of signalling point "X" regarding an inhibited link to signalling point "Y", the following actions take place:

a) A check is performed at signalling point "X" to determine whether an uninhibit message can be sent to signalling point "Y", either over an available route, or if all routes to signalling point "Y" are unavailable, over the concerned inhibited link. If all routes to signalling point "Y" are unavailable and the concerned inhibited link is marked failed or processor outage, management is informed that uninhibiting is not possible.

b) If uninhibiting is possible, signalling point "X" sends an uninhibit signalling link message to signalling point "Y" indicating that the link identified in the message should be uninhibited.

c) Upon receipt of the uninhibit link message, signalling point "Y" returns an uninhibit acknowledgement message to signalling point "X" and cancels the remote inhibit indication. If no local inhibited, failed or blocked condition exists on the link, it is put in the available state and changeback is initiated.

d) On receipt of the uninhibit acknowledgement message, signalling point "X" cancels the local inhibit indication and informs management that the link has been uninhibited. If no remote inhibited, failed or blocked condition exists on the link, it is put in the available state and changeback is initiated.

e) If, for any reason, the uninhibit acknowledgement message is not received, a timer T12 expires. If this is the first expiry of T12 for this uninhibition attempt on this link, the procedure is restarted including inspection of the status of the destination of the unhibit message. If the destination is not available, or T12 has expired for the second time during the uninhibition attempt on this link, management is informed, and the uninhibition is abandoned.

### 10.3.2 *Signalling routing control initiated uninhibiting*

Upon receipt of an uninhibit request from signalling routing control at signalling point "X" regarding an inhibited link to signalling point "Y", the following actions take place:

a) A check is performed at signalling point "X" to determine whether the concerned inhibited link is marked failed or blocked. If it is, then signalling point "X" is unable to transmit an uninhibit message to signalling point "Y", uninhibiting is therefore not possible, and the uninhibiting attempt is abandoned.

b) If uninhibiting is possible, a further check is performed by signalling point "X" to determine whether inhibiting initiated by "X" (local inhibiting) or inhibiting initiated by "Y" (remote inhibiting) is in effect.

c) If local inhibiting is in effect, then the actions described in §§ 10.3.1 b), c), d) and e) take place. If uninhibition is abandoned, step f) below is taken.

d) If remote inhibiting is in effect, then signalling point "X" requests forced uninhibiting of the signalling link by sending a force uninhibit signalling link message to signalling point "Y", which will then initiate uninhibiting in accordance with the description given in §§ 10.3.1 b), c), d) and e).

The force uninhibit signalling link message is transmitted down the link to be uninhibited.

e) If, for any reason, an uninhibit signalling link message is not received in response to the force uninhibit message, a timer T13 expires. If this is the first expiry of T13 for this uninhibition attempt on this link, the procedure is restarted including inspection of the status of the inhibited link. If the link is marked failed or blocked, or timer T13 has expired for the second time during uninhibition of this link, management is informed and the uninhibition is abandoned.

f) If an attempt to uninhibit a signalling link is abandoned, signalling routing control attempts to uninhibit the next inhibited link to signalling point "Y", starting from a) above. The search continues until either a link is successfully uninhibited or all possible links to "Y" in the routing table have been exhausted, or the destination has become available for other reasons.

10.4 *Receipt of unexpected management inhibition messages*

a) An inhibit signalling link message concerning an inhibited signalling link is answered with an inhibit acknowledgement message without taking any further action.

b) An uninhibit signalling link message concerning an uninhibited signalling link is answered with an uninhibit acknowledgement message without taking any further action.

c) A force uninhibit signalling link message concerning an uninhibited link is answered with an uninhibit signalling link message without taking any further action.

d) If an inhibit acknowledgement message is received and no inhibit signalling link message is outstanding for the concerned link, no action is taken.

e) If an uninhibit acknowledgement message is received and no uninhibit signalling link message is outstanding for the concerned link, no action is taken.

10.5 *Management inhibited link status and processor recovery*

a) After a local processor recovery that involves loss of inhibit status information, the signalling point will mark all links as uninhibited, and message traffic will be restarted.

b) If messages for Level 4 are received on an inhibited signalling link, the messages will be discriminated and distributed.

10.6 *Inhibit test procedure*

When a signalling link becomes management inhibited, periodic tests are started to guard the inhibition status at each end of the link.

10.6.1 A local inhibit test is performed when timer T22 expires at signalling point X and the concerned link is marked locally inhibited. In this case a local inhibit test message is sent to the signalling point Y at the other end of the link, and timer T22 is restarted.

Reception of a local inhibit test message causes:

i) no action, if the concerned link is marked remotely inhibited at the receiving signalling point Y or:

ii) the force uninhibit procedure to be invoked at the receiving signalling point Y, if the concerned link is not marked remotely inhibited at Y. This procedure causes the locally inhibited status of the link at X to be cancelled.

If a timer T22 expires and the concerned link is not locally inhibited, no further action is taken.

10.6.2 A remote inhibit test is performed when timer T23 expires at signalling point Y and the concerned link is marked remotely inhibited. In this case a remote inhibit test message is sent to signalling point X at the other end of the link, and timer T23 is restarted.

Reception of a remote inhibit test message causes:

i) no action, if the concerned link is marked locally inhibited at the receiving signalling point X or:

ii) the uninhibit procedure to be invoked at the receiving signalling point X, if the concerned link is not marked locally inhibited at X. This procedure causes the remotely inhibited status of the link at Y to be cancelled.

If a timer T23 expires and the concerned link is not remotely inhibited, no further action is taken.

## 11 Signalling traffic flow control

### 11.1 *General*

The purpose of the signalling traffic flow control function is to limit signalling traffic at its source in the case when the signalling network is not capable of transferring all signalling traffic offered by the user because of network failures or congestion situations.

Flow control action may be taken as a consequence of a number of events; the following cases have been identified:

- Failure in the signalling network (signalling links or signalling points) has resulted in routeset unavailability. In this situation, flow control may provide a short term remedy until more appropriate actions can be taken.
- Congestion of a signalling link or signalling point has resulted in a situation where reconfiguration is not appropriate.
- Failure of a part has made it impossible for the user to handle messages delivered by the Message Transfer Part.

When the normal transfer capability is restored, the flow control functions initiate resumption of the normal traffic flow.

### 11.2 *Flow control indications*

The need for the following indications has been identified.

#### 11.2.1 *Signalling route set unavailability*

In the case when no signalling route is available for traffic towards a particular destination (see §§ 5.3.3 and 7.2.3) an indication is given from the Message Transfer Part to the local user parts informing them that signalling messages destined to the particular signalling point cannot be transferred via the signalling network. Each user then takes appropriate actions in order to stop generation of signalling information destined for the inaccessible signalling point.

#### 11.2.2 *Signalling route set availability*

In the case when a signalling route becomes available for traffic to a previously unavailable destination (see §§ 6.2.3 and 8.2.3), an indication is given from the Message Transfer Part to the local user parts informing them that signalling messages destined to the particular signalling point can be transferred via the signalling network. Each user then takes appropriate actions in order to start generation of signalling information destined for the now accessible signalling point.

#### 11.2.3 *Signalling route set congestion (International signalling network)*

11.2.3.1 When the congestion status of a signalling route set changes to congested, the following actions will be taken:

i) When a message signal unit from a local User Part is received for a congested route set the following actions are performed:

   a) The MSU is passed to level 2 for transmission.

   b) A congestion indication primitive will be returned to each level 4 User Part, for the initial message and for at least every $n$ messages ($n = 8$) received for the congested destination. The congestion indication primitive contains as a parameter the DPC of the affected destination.

ii) When a message signal unit is received at an STP for a congested route set, the following actions take place:

a) The MSU is passed to level 2 for transmission.

b) A transfer controlled message is sent to the originating point for the initial message and for every $n$ messages ($n = 8$) received from any originating point for the congested route set or for every link of the congested route set or for every linkset of the congested route set.

11.2.3.2 After the reception of a transfer controlled message, the receiving signalling point informs each level 4 User Part of the affected destination by means of a congestion indication primitive specified in § 11.2.3.1 i).

11.2.3.3 When the status of a signalling route set changes to uncongested, normal operation is resumed. Resumption of message transmission towards the concerned destination is the responsibility of the level 4 User Parts.

11.2.4 *Signalling route set congestion (National option with congestion priorities)*

In the case when the congestion status of a signalling route set changes as a result of either the receipt of a transfer controlled message relating to a particular destination (see § 13.7) or an indication of local signalling link congestion, or due to the signalling route-set-congestion-test procedure (see § 13.9) an indication is given from the Message Transfer Part to the local level 4 informing it about the current congestion status of the signalling route set. Each user then takes appropriate actions in order to stop generation of signalling messages destined for the affected signalling point with congestion priorities lower than the specified congestion status. Messages received from the local level 4 with congestion priorities lower than the current signalling route set congestion status are discarded by the Message Transfer Part.

11.2.5 *Signalling route set congestion (National options without congestion priorities)*

For national signalling networks using multiple signalling link congestion states without congestion priority, $S + 1 (1 \leqslant S \leqslant 3)$ levels of route set congestion status are provided.

The procedure is the same as that specified in § 11.2.3, except that the congestion indication primitive contains the congestion status as a parameter in addition to the DPC of the affected destination.

11.2.6 *Signalling point/signalling transfer point congestion*

The detection of congestion onset and abatement in a signalling point or signalling transfer point should, if required, be implementation dependent. Any resulting action taken, and messages and primitives sent, should align with those procedures, messages and primitives specified for signalling route set congestion.

11.2.7 *MTP user flow control*

If the Message Transfer Part is unable to distribute a received message to a local User Part because that User Part is unavailable, (User Part unavailability is an implementation dependent notion), the Message Transfer Part sends a User Part Unavailable (UPU) message to the Message Transfer Part at the originating signalling point.

When the originating signalling point's Message Transfer Part receives a User Part Unavailable message, it:

a) informs the management process,

b) sends an indication (MTP-STATUS with the appropriate parameters) to the affected local User Part informing it that that User Part at the particular remote signalling point is unavailable.

The user should then take appropriate action in order to stop generation of signalling information for the unavailable User Part.

The User Part Unavailable message contains:

- the label, indicating the destination and originating points;
- the user part unavailable signal;
- the identity of the unavailable user part.

The format and coding of this message appear in § 15.

When the Message Transfer Part is again able to distribute received messages to a previously unavailable local User Part, that Message Transfer Part delivers the received messages to that User Part.

### 11.2.8 *User part congestion*

User part congestion procedures in the MTP are for further study.

## 12 Signalling link management

### 12.1 *General*

12.1.1 The signalling link management function is used to control the locally connected signalling links. The function provides means for establishing and maintaining a certain predetermined capability of a link set. Thus, in the event of signalling link failures the signalling link management function controls actions aimed at restoring the capability of the link set.

Three sets of signalling link management procedures are specified in the following sections. Each set corresponds to a certain level of automation as regards allocation and reconfiguration of signalling equipment. The basic set of signalling link management procedures (see § 12.2) provides no automatic means for allocation and reconfiguration of signalling equipment. The basic set includes the minimum number of functions which must be provided for international application of the signalling system.

Two alternative sets of signalling link management procedures are provided as options and include functions allowing for a more efficient use of signalling equipment in the case when signalling terminal devices have switched access to signalling data links.

12.1.2 A signalling link set consists of one or more signalling links having a certain order of priority as regards the signalling traffic conveyed by the link set (see § 4). Each signalling link in operation is assigned a signalling data link and a signalling terminal at each end of the signalling data link.

The signalling link identity is independent of the identities of the constituent signalling data link and signalling terminals. Thus, the identity referred to by the Signalling Link Code (SLC) included in the label of messages originated at Message Transfer Part level 3 is the signalling link identity and not the signalling data link identity or the signalling terminal identity.

Depending on the level of automation in an application of the signalling system, allocation of signalling data link and signalling terminals to a signalling link may be made manually or automatically.

In the first case, applicable for the basic signalling link management procedures, a signalling link includes predetermined signalling terminals and a predetermined signalling data link. To replace a signalling terminal or signalling data link, a manual intervention is required. The signalling data link to be included in a particular signalling link is determined by bilateral agreement (see also Recommendation Q.702).

In the second case for a given signalling point, a signalling link includes any of the signalling terminals and any of the signalling data links applicable to a *link group.* As a result of, for example, signalling link failure, the signalling terminal and signalling data link included in a signalling link, may be replaced automatically. The criteria and procedures for automatic allocation of signalling terminals and signalling data links are specified in §§ 12.5 and 12.6 respectively. The implementation of these functions requires that for a given link group any signalling terminal can be connected to any signalling data link.

*Note* – A link group is a group of identical signalling links directly connecting two signalling points. A link set may include one or more link groups.

12.1.3 When a link set is to be brought into service, actions are taken to establish a predetermined number of signalling links. This is done by connecting signalling terminals to signalling data links and for each signalling link performing an initial alignment procedure (see Recommendation Q.703, § 7.3). The process of making a signalling link ready to carry signalling traffic is defined as *signalling link activation.*

Activation of a signalling link may also be applicable, for example when a link set is to be extended or when a persisting failure makes another signalling link in the link set unavailable for signalling traffic.

In the case of signalling link failure, actions should be taken to restore the faulty signalling link, i.e. to make it available for signalling again. The restoration process may include replacement of a faulty signalling data link or signalling terminal.

A link set or single signalling link is taken out of service by means of a procedure defined as *signalling link deactivation.*

The procedures for activation, restoration and deactivation are initiated and performed in different ways depending on the level of automation applicable for a particular implementation of the signalling system. In the following, procedures are specified for the cases when:

a) no automatic functions are provided for allocation of signalling terminals and signalling data links (see § 12.2).

b) an automatic function is provided for allocation of signalling terminals (see § 12.3).

c) automatic functions are provided for allocation of signalling terminals and signalling data links (see § 12.4).

## 12.2 *Basic signalling link management procedures*

### 12.2.1 *Signalling link activation*

12.2.1.1 In the absence of failures, a link set contains a certain predetermined number of active (i.e. aligned) signalling links. In addition, the link set may contain a number of inactive signalling links, i.e. signalling links which have not been put into operation. Predetermined signalling terminals and a signalling data link are associated with each inactive signalling link.

The number of active and inactive signalling links in the absence of failures, and the priority order for the signalling links in a link set, should be identical at both ends of the link set.

*Note* – In the typical case, all signalling links in a link set are active in the absence of failures.

12.2.1.2 When a decision is taken to activate an inactive signalling link, initial alignment starts. If the initial alignment procedure is successful, the signalling link is active and a signalling link test is started. If the signalling link test is successful the link becomes ready to convey signalling traffic. In the case when initial alignment is not possible, as determined at Message Transfer Part level 2 (see Recommendation Q.703, § 7), new initial alignment procedures are started on the same signalling link after a time T17 (delay to avoid the oscillation of initial alignment failure and link restart. The value of T17 should be greater than the loop delay and less than timer T2, see Recommendation Q.703, § 7.3). If the signalling link test fails, link restoration starts until the signalling link is activated or a manual intervention is made.

### 12.2.2 *Signalling link restoration*

After a signalling link failure is detected, signalling link initial alignment will take place. In the case when the initial alignment procedure is successful, a signalling link test is started. If the signalling link test is successful the link becomes restored and thus available for signalling.

If initial alignment is not possible, as determined at Message Transfer Part level 2 (see Recommendation Q.703, § 7), new initial alignment procedures may be started on the same signalling link after a time T17 until the signalling link is restored or a manual intervention is made e.g. to replace the signalling data link or the signalling terminal.

If the signalling link test fails, the restoration procedure is repeated until the link is restored or a manual intervention made.

12.2.3 *Signalling link deactivation*

An active signalling link may be made inactive by means of a deactivation procedure, provided that no signalling traffic is carried on that signalling link. When a decision has been taken to deactivate a signalling link the signalling terminal of the signalling link is taken out of service.

12.2.4 *Link set activation*

A signalling link set not having any signalling links in service is started by means of a link set activation procedure. Two alternative link set activation procedures are defined:

- link set normal activation,
- link set emergency restart.

12.2.4.1 *Link set normal activation*

Link set normal activation is applicable when a link set is to be put into service for the first time (link set initial activation) or when a link set is to be restarted (link set normal restart); the latter is applicable for example in the case when:

- all signalling links in a link set are faulty,
- a processor restart in a signalling point makes it necessary to re-establish a link set,
- a signalling point recognizes other irregularities concerning the interworking between the two signalling points,

provided that none of the above events create an emergency situation.

When link set normal activation is initiated, signalling link activation starts on as many signalling links as possible. (All signalling links in the link set are regarded as being inactive at the start of the procedure.)

The signalling link activation procedures are performed on each signalling link in parallel as specified in § 12.2.1 until the signalling links are made active.

Signalling traffic may, however, commence when one signalling link is successfully activated.

12.2.4.2 *Link set emergency restart*

Link set emergency restart is applicable when an immediate reestablishment of the signalling capability of a link set is required, (i.e. in a situation when the link set normal restart procedure is not fast enough). The precise criteria for initiating link set emergency restart instead of normal restart may vary between different applications of the signalling system. Possible situations for emergency restart are, for example:

- when signalling traffic that may be conveyed over the link set to be restarted is blocked,
- when it is not possible to communicate with the signalling point at the remote end of the link set.

When link set emergency restart is initiated, signalling link activation starts on as many signalling links as possible, in accordance with the principles specified for normal link set activation. In this case, the signalling terminals will have emergency status (see Recommendation Q.703, § 7) resulting in the sending of status indications of type "E" when applicable. Furthermore, the signalling terminals employ the emergency proving procedure and short time-out values in order to accelerate the procedure.

When the emergency situation ceases, a transition from emergency to normal signalling terminal status takes place resulting in the employment of the normal proving procedure and normal time-out values.

12.2.4.3 *Time-out values*

The initial alignment procedure (specified in Recommendation Q.703, § 7.3) includes time-outs the expiry of which indicates the failure of an activation or restoration attempt.

## 12.3 *Signalling link management procedures based on automatic allocation of signalling terminals*

### 12.3.1 *Signalling link activation*

12.3.1.1 In the absence of failures a link set contains a certain predetermined number of active (i.e. aligned) signalling links. The link set may also contain a number of inactive signalling links.

An inactive signalling link is a signalling link not in operation. A predetermined signalling data link is associated with each inactive signalling link; however, signalling terminals may not yet be allocated.

The number of active and inactive signalling links in the absence of failures, and the priority order for the signalling links in a link set, should be identical at both ends of the link set.

12.3.1.2 Whenever the number of active signalling links is below the value specified for the link set, actions to activate new inactive signalling links should be taken automatically. This is applicable, for example, when a link set is to be brought into service for the first time (see § 12.3.4) or when a link failure occurs. In the latter case, activation starts when the restoration attemps on the faulty link are considered unsuccessful (see § 12.3.2).

The signalling link(s) to activate is the inactive link(s) having the highest priority in the link set.

Generally, if it is not possible to activate a signalling link, an attempt to activate the next inactive signalling link (in priority order) is made. In the case when an activation attempt performed on the last signalling link in the link set is unsuccessful, the "next" signalling link is the first inactive signalling link in the link set (i.e. there is a cyclic assignment).

Activation of a signalling link may also be initiated manually.

Activation shall not be initiated automatically for a signalling link previously deactivated by means of a manual intervention.

12.3.1.3 When a decision is taken to activate a signalling link, the signalling terminal to be employed has to be allocated at each end.

The signalling terminal is allocated automatically by means of the function defined in § 12.5.

In the case when the automatic allocation function cannot provide a signalling terminal the activation attempt is aborted.

The predetermined signalling data link which may be utilized for other purposes when not connected to a signalling terminal must be removed from its alternative use (e.g. as a speech circuit) before signalling link activation can start.

12.3.1.4 The chosen signalling terminal is then connected to the signalling data link and initial alignment starts (see Recommendation Q.703, § 7).

If the initial alignment procedure is successful, the signalling link is active and a signalling link test is started. If the signalling link test is successful the link becomes ready to convey signalling traffic.

If initial alignment is not possible, as determined at Message Transfer Part level 2 (see Recommendation Q.703, § 7), the activation is unsuccessful and activation of the next inactive signalling link (if any) after a time T17 is initiated. Successive initial alignment attempts may, however, continue on the previous (faulty) signalling link after a time T17 until it is restored or its signalling terminal is disconnected (see § 12.5).

In view of the fact that if it is not possible to activate a signalling link an attempt is made to activate the next inactive signalling link in a link set, it may be that the two ends of a link set continuously attempt to activate different signalling links. By having different values of initial alignment time out T2 at the two ends of the link set (see § 12.3.4.3) it is ensured that eventually both ends of the link set will attempt to activate the same signalling link.

12.3.2 *Signalling link restoration*

12.3.2.1 After a signalling link failure is recognized, signalling link initial alignment will take place (see Recommendation Q.703, § 7). In the case when the initial alignment is successful, a signalling link test is started. If the signalling link test is successful the link becomes restored and thus available for signalling. If the initial alignment is unsuccessful or the test fails, the signalling terminals and signalling link may be faulty and require replacement.

12.3.2.2 The signalling terminal may be automatically replaced in accordance with the principles defined for automatic allocation of signalling terminals (see § 12.5). After the new signalling terminal has been connected to the signalling data link, signalling link initial alignment starts. If successful, the signalling link is restored.

If initial alignment is not possible or if no alternative signalling terminal is available for the faulty signalling link, activation of the next signalling link in the link set (if any) starts. In the case when it is not appropriate to replace the signalling terminal of the faulty signalling link (e.g. because it is assumed that the signalling data link is faulty) activation of the next inactive signalling link (if any) is also initiated. In both cases successive initial alignment attempts may continue on the faulty signalling link after a time T17 until a manual intervention is made or the signalling terminal is disconnected (see § 12.5).

*Note* – In the case when a signalling terminal cannot be replaced, activation of the next signalling link is only initiated if the link set includes an alternative link group having access to signalling terminals other than the one used by the signalling link for which restoration is not possible.

12.3.3 *Signalling link deactivation*

In the absence of failures a link set contains a specified number of active (i.e. aligned) signalling links. Whenever that number is exceeded (e.g. as a result of signalling link restoration), the active signalling link having the lowest priority in the link set is to be made inactive automatically provided that no signalling traffic is carried on that signalling link.

Deactivation of a particular signalling link may also be initiated manually, for example in conjunction with manual maintenance activities.

When a decision has been taken to deactivate a signalling link, the signalling terminal and signalling data link may be disconnected.

After deactivation, the idle signalling terminal may become part of other signalling links (see § 12.5).

12.3.4 *Link set activation*

A signalling link set not having any signalling links in service is started by means of a link set activation procedure. The objective of the procedure is to activate a specified number of signalling links for the link set. The activated signalling links should, if possible, be the signalling links having the highest priority in the link set. Two alternative link set activation procedures are defined:

- link set normal activation,
- link set emergency restart.

12.3.4.1 *Link set normal activation*

Link set normal activation is applicable when a link set is to be put into service for the first time (link set initial activation) or when a link set is to be restarted (link set normal restart); the latter is applicable, for example, in the case when:

- all signalling links in a link set are faulty;
- a processor restart in a signalling point makes it necessary to re-establish a link set;
- a signalling point recognizes other irregularities concerning the interworking between the two signalling points, e.g. that a certain signalling data link is associated with different signalling links at the two ends of the link set;

provided that none of the above events create an emergency situation.

When link set normal activation is initiated, signalling link activation starts on as many signalling links as possible. (All signalling links in the link set are regarded as being inactive at the start of the procedure). If activation cannot take place on all signalling links in the link set (e.g., because a sufficient number of signalling terminals is not available), then the signalling links to activate are determined in accordance with the link priority order.

*Note* – All idle signalling terminals may not necessarily be made available for link set activation. Thus making possible, for example, restoration of faulty signalling links in other link sets at the same time.

The signalling link activation procedures are performed as specified in § 12.3.1.

If the activation attempt for a signalling link is unsuccessful (i.e. initial alignment is not possible), activation of the next inactive signalling link, if any, in the priority order is initiated. (Inactive links exist in the case when the number of signalling terminals available is less than the number of signalling links defined for the link set). According to the principles for automatic allocation of signalling terminals defined in § 12.5, the signalling terminal connected to the unsuccessfully activated signalling link will typically be connected to the signalling data link of that signalling link for which the new activation attempt is to be made.

When a signalling link is successfully activated, signalling traffic may commence.

After the successful activation of one signalling link, the activation attempts on the remaining signalling links continue in accordance with the principles defined in § 12.3.1, in such a way that the signalling links having the highest priorities are made active. This is done in order to obtain, if possible, the normal configuration within the link set. Signalling link activation continues until the predetermined number of active signalling links is obtained.

#### 12.3.4.2 *Link set emergency restart*

Link set emergency restart is applicable in the case the link set normal restart procedure is not fast enough. Emergency restart is performed in the same way as link set normal activation except that, in the case of emergency restart, the emergency proving procedure and the short emergency time-out values (see Recommendation Q.703, § 7) are employed in order to accelerate the procedure (see further § 12.2.4.2).

#### 12.3.4.3 *Time-out values*

The values of the initial alignment time-out T2 (see Recommendation Q.703, § 7) will be different at the two ends of the link set, if automatic allocation of signalling terminals or signalling data links is applied at both ends of a signalling link set.

### 12.4 *Signalling link management procedures based on automatic allocation of signalling data links and signalling terminals*

#### 12.4.1 *Signalling link activation*

12.4.1.1 In the absence of failures a link set contains a certain predetermined number of active (i.e. aligned) signalling links. The link set may also contain a number of inactive signalling links.

An inactive signalling link is a signalling link currently not in operation. It is not associated with any signalling terminal or signalling data link (i.e. the signalling link is only identified by its position in the link set).

The number of active and inactive signalling links (in the absence of failures), and the priority order for the signalling links in a link set, should be identical at both ends of the link set.

12.4.1.2 Whenever the number of active signalling links is below the value specified for the link set, actions to activate new inactive signalling links should be taken automatically. This is, for example, applicable when a link set is to be brought into service for the first time (see § 12.4.4) or when a link failure occurs. In the latter case, activation starts when the restoration attempts on the faulty link are considered unsuccessful (see § 12.4.2).

The signalling link(s) to activate is the inactive link(s) having the highest priority in the link set.

If it is not possible to activate a signalling link an attempt to activate the next inactive signalling link (in priority order) is made. In the case when an activation attempt performed on the last signalling link in the link set is unsuccessful, the "next" signalling link is the first inactive link in the link set (i.e. a cyclic assignment).

*Note* – Activation of the next signalling link is only initiated if the link set includes an alternative link group, having access to other signalling terminals and/or other signalling data links than the signalling link for which activation is not possible.

Activation of a particular signalling link may also be initiated upon receiving a request from the remote signalling point, or by a manual request.

Activation shall not be initiated automatically for a signalling link previously inactivated by means of a manual intervention.

12.4.1.3 When a decision is taken to activate a signalling link, the signalling terminals and signalling data link to be employed have to be allocated.

A signalling terminal is allocated automatically by means of the function defined in § 12.5.

The signalling data link is allocated automatically by means of the function defined in § 12.6. However, in conjunction with link set activation the identity of the signalling data link to use may be predetermined (see further § 12.4.4). A signalling data link which is not connected to a signalling terminal may be utilized for other purposes, e.g. as a speech circuit. When the data link is to be employed for signalling, it must be removed from its alternative use.

In the case when the automatic allocation functions cannot provide a signalling terminal or a signalling data link, the activation attempt is aborted.

12.4.1.4 When the signalling data link and signalling terminal to be used for a particular signalling link are determined, the signalling terminal is connected to the signalling data link and signalling link initial alignment starts (see Recommendation Q.703, § 7). If the initial alignment procedure is successful, the signalling link is active and a signalling link test is started. If the signalling link test is successful the link becomes ready to convey signalling traffic.

If initial alignment is not possible, as determined at Message Transfer Part level 2 (see Recommendation Q.703, § 7), alternative signalling data links are automatically connected to the signalling terminal, until an initial alignment procedure is successfully completed. In the case when the function for automatic allocation of signalling data links cannot provide an alternative signalling data link, the activation is regarded as unsuccessful and activation of the next inactive signalling link (if any) is initiated (see, however, the Note to § 12.4.1.2 above). Successive initial alignment attempts may continue on the previous signalling link after a time T17 until it is activated or its signalling terminal is disconnected (see § 12.5).

12.4.2 *Signalling link restoration*

12.4.2.1 After a signalling link failure is recognized, signalling link initial alignment will take place (see Recommendation Q.703, § 7). In the case when the initial alignment is successful, a signalling link test is started. If the signalling link test is successful the link becomes restored and thus available for signalling.

If the initial alignment is unsuccessful or if the test fails the signalling terminal and signalling data link may be faulty and require replacement.

12.4.2.2 The signalling data link may be automatically replaced by an alternative, in accordance with the principles defined in § 12.6. After the new signalling data link has been connected to the signalling terminal, signalling link initial alignment starts. If successful, the signalling link is restored. If not, alternative data links are connected to the signalling terminal, until an initial alignment procedure is successfully completed.

If the automatic allocation function cannot provide a new signalling data link, activation of the next inactive signalling link (if any) is initiated (see, however, the Note to § 12.4.1.2). Successive initial alignment attempts may, however, continue on the previous (faulty) signalling link after a time T17 until it is restored or its signalling terminal is disconnected.

12.4.2.3 The signalling terminal may be automatically replaced in accordance with the principles defined in § 12.5. After the new signalling terminal has been connected to the signalling data link, signalling link initial alignment starts. If successful, the signalling link is restored. If not, activation of the next signalling link in the link set (if any) starts (see, however, the Note to § 12.4.1.2).

Successive initial alignment attempts may, however, continue on the previous (faulty) signalling link after a time T17 until it is restored or, for example, the signalling terminal or signalling data link is disconnected.

*Note* – Activation of the next signalling link in the link set should not be initiated as long as one of the activities described in §§ 12.4.2.2 and 12.4.2.3 above is taking place.

### 12.4.3 *Signalling link deactivation*

In the absence of failures, a link set contains a specified number of active (i.e. aligned) signalling links. Whenever that number is exceeded (e.g. as a result of signalling link restoration) the active signalling link having the lowest priority in the link set is to be made inactive automatically, provided that no signalling traffic is carried on that signalling link.

Deactivation of a particular signalling link may also be initiated manually, e.g. in conjunction with manual maintenance activities.

When a decision has been taken to deactivate a signalling link, the signalling terminal and signalling data link may be disconnected. After deactivation the idle signalling terminal and signalling data link may become parts of other signalling links (see §§ 12.5 and 12.6).

### 12.4.4 *Link set activation*

Link set activation is applicable in the case when a link set not having any signalling links in service is to be started for the first time or after a failure (see § 12.3.4). The link set activation procedure is performed as specified in § 12.3.4, also as regards the allocation of signalling data links, i.e. signalling data links are allocated in accordance with predetermined list assigning a signalling data link to some or all of the signalling links in the link set. This is done in order to cater for the situation when it is not possible to communicate with the remote end of the link set (see § 12.6). However, when a signalling link has become active, signalling data link allocation may again be performed automatically (i.e. activation of a signalling link takes place as specified in § 12.4.1).

## 12.5 *Automatic allocation of signalling terminals*

In conjunction with the signalling link activation and restoration procedures specified in §§ 12.3 and 12.4, signalling terminals may be allocated automatically to a signalling link. A signalling terminal applicable to the link group is allocated in accordance with the following principles:

a) an idle signalling terminal (i.e. a signalling terminal not connected to a signalling data link) is chosen if possible;

b) if no idle signalling terminal is available, a signalling terminal is chosen which is connected to an unsuccessfully restored or activated signalling link.

*Note* – Activation and restoration is regarded as unsuccessful when it is not possible to complete the initial alignment procedure successfully (see §§ 12.3 and 12.4).

Measures should be employed to ensure that signalling terminal to be allocated to signalling links are able to function correctly (see Recommendation Q.707).

A link set may by assigned a certain number of signalling terminals. A signalling terminal may be transferred from a signalling link in one link set to a signalling link in another set [in accordance with b) above] only when the remaining number of signalling terminals in the link set is not below the specified value.

*Note* – From a link set with a minimum number of signalling terminals, only one signalling terminal and signalling data link may be removed at a time (e.g. for testing, see Recommendation Q.707).

## 12.6 *Automatic allocation of signalling data links*

12.6.1 In conjunction with the signalling link activation and restoration procedures specified in § 12.4, signalling data links may be allocated automatically. Any signalling data link applicable to a link group may be chosen for a signalling link within that link group.

The signalling data links applicable to a link group are determined by bilateral agreement and may, for example, include all speech circuits between two exchanges. A signalling data link may also be established as a semipermanent connection via one or more intermediate exchanges.

When a potential signalling data link is not employed for signalling, it is normally used for other purposes (e.g. as a speech circuit).

The identity of the signalling data link to be used for a particular signalling link is determined at one of the two involved signalling points and reported to the remote end by a signalling data link connection order message. The signalling point controlling the choice of signalling data link is the signalling point initiating the activation or restoration procedure or, in the case when both ends initiate the procedure at the same time, the signalling point having the highest signalling point code (included in the label of the message).

12.6.2 When a signalling data link has been chosen at a signalling point, the data link is made unavailable for other uses (e.g. as a speech circuit) and an order to connect the appointed signalling data link to a signalling terminal is sent to the signalling point at the remote end of the signalling link.

The signalling-data-link-connection-order message contains:

- the label, indicating the destination and originating signalling points and the identity of the signalling link to activate or restore;
- the signalling-data-link-connection-order;
- the identity of the signalling data link.

Formats and codes for the signalling-data-link-connection-order message appear in § 15.

12.6.3 Upon reception of the signalling-data-link-connection-order, the following applies:

a) In the case when the signalling link to which a received signalling-data-link-connection-order message refers is inactive as seen from the receiving signalling point, the message is regarded as an order to activate the concerned signalling link, resulting in, for example, allocation of a signalling terminal. The signalling data link indicated in the signalling-data-link-connection-order is then connected to the associated signalling terminal and signalling link initial alignment starts. An acknowledgement is sent to the remote signalling point.

   If it is not possible to connect the appointed signalling data link to a signalling terminal (e.g. because there is no working signalling terminal available), the acknowledgement contains an indication informing the remote signalling point whether or not an alternative signalling data link should be allocated to the concerned signalling link.

b) If the signalling point receives a signalling-data-link-connection-order when waiting for an acknowledgement, the order is disregarded in the case when the signalling point code of the receiving signalling point is higher than the signalling point code of the remote signalling point. If the remote signalling point has the higher signalling point code, the message is acknowledged and the signalling data link referred to in the received message is connected.

c) If a signalling-data-link-connection-order is received in other situations (e.g. in the case of an error in procedure), no actions are taken.

The signalling-data-link-connection-acknowledgement contains the label, indicating the destination and originating signalling points and the identity of the signalling link to activate or restore, and one of the following signals:

- connection-successful signal, indicating that the signalling data link has been connected to a signalling terminal;
- connection-not-successful signal, indicating that it was not possible to connect the signalling data link to a signalling terminal, and that an alternative signalling data link should be allocated;
- connection-not-possible signal, indicating that it was not possible to connect the signalling data link to a signalling terminal, and that no alternative signalling data link should be allocated.

The formats and codes for the signalling data link connection acknowledgement message appear in § 15.

12.6.4 When the signalling point initiating the procedure receives a message indicating that signalling data link and signalling terminal have been connected at the remote end, the signalling data link is connected to the associated signalling terminal and initial alignment starts (see § 12.4).

If the acknowledgement indicates that it was not possible to connect the signalling data link to a signalling terminal at the remote end, an alternative signalling data link is allocated and a new signalling-data-link-connection-order is sent (as specified above). However, if the acknowledgement indicates that no alternative signalling data link should be allocated, the activation or restoration procedure is terminated for the concerned signalling link.

If no signalling-data-link-connection-acknowledgement or order is received from the remote signalling point within a time T7 (see § 16), the signalling-data-link-connection-order is repeated.

12.6.5 When a signalling data link is disconnected in conjunction with signalling link restoration or deactivation, the signalling data link is made idle (and available, e.g. as a speech circuit).

### 12.7 *Different signalling link management procedures at the two ends of a link set*

Normally both ends of a link set will use the same signalling link management procedures.

However, if one end uses the basic signalling link management procedures, the other end may use the signalling link management procedures based on automatic allocation of signalling terminals. In that case a signalling link includes a predetermined signalling terminal at one end, a predetermined signalling data link and at the other end, any of the signalling terminals applicable to the concerned link group.

If one end of a link set uses the basic signalling link management procedures and the other end uses the signalling link management procedures based on automatic allocation of signalling terminals, the values of the initial alignment time-out T2 do not have to be different at the two ends of the link set.

## 13 Signalling route management

### 13.1 *General*

The purpose of the signalling route management function is to ensure a reliable exchange of information between the signalling points about the availability of the signalling routes.

The unavailability, restriction[15] and availability of a signalling route is communicated by means of the transfer-prohibited, transfer-restricted[15] and transfer allowed procedures, respectively in §§ 13.2, 13.4 and 13.3.

Recovery of signalling route status information is made by means of the signalling-route-set-test procedure specified in § 13.5.

In the international signalling network, congestion of a route set is communicated by means of the transfer-controlled (TFC) messages specified in § 13.6.

In national networks, congestion of a signalling route set may be communicated by means of the TFC as specified in §§ 13.7 and 13.8 and the signalling route set congestion test procedure specified in § 13.9.

### 13.2 *Transfer prohibited*

13.2.1 The transfer-prohibited procedure is performed at a signalling point acting as a signalling transfer point for messages relating to a given destination, when it has to notify one or more adjacent signalling points that they must no longer route the concerned messages via that signalling transfer point.

---

[15] National option.

The transfer-prohibited procedure makes use of the transfer-prohibited message which contains:

- the label, indicating the destination and originating points;
- the transfer-prohibited signal; and
- the destination for which traffic transfer is no longer possible.

Format and code of these messages appear in § 15.

Transfer prohibited messages are always addressed to an adjacent signalling point. They may use any available signalling route that leads to that signalling point.[16)]

13.2.2 A transfer-prohibited message relating to a given destination X is sent from a signalling transfer point Y in the following cases:

i) When signalling transfer point Y starts to route (at changeover, changeback, forced or controlled rerouting) signalling destined to signalling point X via a signalling transfer point Z not currently used by signalling transfer point Y for this traffic. In this case the transfer-prohibited message is sent to signalling transfer point Z.

ii) When signalling transfer point Y recognizes that it is unable to transfer signalling traffic destined to signalling point X (see §§ 5.3.3 and 7.2.3). In this case a transfer-prohibited message is sent to all accessible adjacent signalling points (Broadcast method).

iii) When a message destined to signalling point X is received at signalling transfer point Y and Y is unable to transfer the message. In this case the transfer prohibited message is sent to the adjacent signalling point from which the message concerned was received (Response Method).

iv) When an adjacent signalling point Z becomes accessible, STP Y sends to Z a transfer prohibited message concerning destination X, if X is inaccessible from Y (see § 9).

v) When a signalling transfer point Y restarts, it broadcasts to all accessible adjacent signalling points transfer prohibited messages concerning destination X, if X is inaccessible from Y (see § 9).

As long as transfer-prohibited messages for a destination are being transmitted according to criteria i), ii), iv), or v) above, and also within T8 (see § 16) after the last transfer-prohibited message was transmitted, no transfer-prohibited messages will be sent via the Response Method (criterion iii) above) referring to that destination.

Examples of the above situation appear in Recommendation Q.705.

13.2.3 When a signalling point receives a transfer-prohibited message from signalling transfer point Y it performs the actions specified in § 7 (since reception of transfer-prohibited message indicates the unavailability of the concerned signalling route, see § 3.4.1). In other words, it may perform forced re-routing and, if appropriate, generate additional transfer-prohibited messages.

13.2.4 In some circumstances it may happen that a signalling point receives either a repeated transfer-prohibited message relating to a nonexistent route (i.e. there is no route from that signalling point to the concerned destination via signalling transfer point Y, according to the signalling network configuration) or to a destination which is already inaccessible, due to previous failures; in this case no actions are taken.

### 13.3 *Transfer allowed*

13.3.1 The transfer-allowed procedure is performed at a signalling point, acting as signalling transfer point for messages relating to a given destination, when it has to notify one or more adjacent signalling points that they may start to route to it, if appropriate, the concerned messages.

The transfer-allowed procedure makes use of the transfer-allowed message which contains:

- the label, indicating the destination and originating points;
- the transfer-allowed signal; and
- the destination for which transfer is now possible.

---

[16)] The possibility of referring to a more general destination than a single signalling point (e.g. a signalling region), or more restrictive destination than a signalling point is for further study.

The format and code of these messages appear in § 15.

Transfer allowed messages are always addressed to an adjacent signalling point. They may use any available signalling route that leads to that signalling point.[17]

13.3.2 A transfer-allowed message relating to a given destination "X" is sent from signalling transfer point "Y" in the following cases:

i) When signalling transfer point "Y" stops routing (at changeback or controlled rerouting) signalling traffic destined to signalling point "X" via a signalling transfer point "Z" (to which the concerned traffic was previously diverted as a consequence of changeover or forced rerouting). In this case the transfer-allowed message is sent to signalling transfer point "Z".

ii) When signalling transfer point "Y" recognizes that it is again able to transfer signalling traffic destined to signalling point "X" (see §§ 6.2.3 and 8.2.3). In this case a transfer-allowed message is sent to all accessible adjacent signalling points. (Broadcast method).

Examples of the above situations appear in Recommendation Q.705.

13.3.3 When a signalling point receives a transfer-allowed message from signalling transfer point "Y", it performs the actions specified in § 8 (since reception of a transfer-allowed message indicates the availability of the concerned signalling route, (see § 3.4.2)). In other words, it may perform controlled re-routing and, if appropriate, generate additional transfer-allowed messages.

13.3.4 In some circumstances it may happen that a signalling point receives either a repeated transfer-allowed message or a transfer-allowed message relating to a non-existent signalling route (i.e. there is no route from that signalling point to the concerned destination via signalling transfer point Y according to the signalling network configuration); in this case no actions are taken.

13.4 *Transfer-restricted (National option)*

13.4.1 The transfer restricted procedure is performed at a signalling point acting as a signalling transfer point for messages relating to a given destination, when it has to notify one or more adjacent signalling points that they should, if possible, no longer route the concerned messages via the signalling transfer point.

The transfer-restricted procedure makes use of the transfer-restricted message which contains:

- the label, indicating the destination and originating points;
- the transfer-restricted signal, and
- the destination for which traffic is no longer desirable.

Formats and codes of this message appear in § 15.

Transfer restricted messages are always adressed to an adjacent signalling point. They may use any available signalling route that leads to that signalling point.

*Note* – Undesirable situations result in increased signalling delays, possibly overloading portions of the network. These inefficiencies could be avoided if the traffic can be appropriately diverted.

13.4.2 A transfer-restricted message relating to a given destination "X" is sent from a signalling transfer point "Y" when the normal link set (combined link set) used by signalling point "Y" to route to destination "X" experiences a long-term failure such as an equipment failure, or there is congestion on an alternate link set currently being used to destination "X". In this case, a transfer-restricted message is sent to all accessible adjacent signalling points.

When an adjacent signalling point "X" becomes accessible, the STP "Y" sends to "X" transfer-restricted messages concerning destinations that are restricted from "Y" (see § 9).

When a signalling point Y restarts, it broadcasts to all accessible adjacent signalling points transfer restricted messages concerning destinations restricted from "Y" (see § 9).

*Note* – Characterization of long term failure remains for further study.

---

[17] The possibility of referring to a more general destination than a single signalling point (e.g. a signalling region), or a more restrictive destination than a single signalling point is for further study.

13.4.3 When a signalling point receives a transfer-restricted message from signalling transfer point "Y" and has an alternative equal priority link set available and not restricted to destination "X", it performs the actions in § 8.2. In other words, it performs controlled rerouting to maintain the sequence of messages while diverting them to the alternative link set. If it cannot perform alternate routing to destination "X" because no alternative link set is available, it may generate additional transfer-restricted messages.

13.4.4 In some circumstances, it may happen that a signalling point receives either a repeated transfer-restricted message or a transfer-restricted message relating to a non-existent route (i.e. there is no route from that signalling point to the concerned destination via signalling transfer point "Y", according to the signalling network configuration); in this case, no actions are taken.

13.4.5 When a transfer-restricted message is received updating a transfer-prohibited status, signalling traffic management decides if an alternative route is available or restricted; if it is not (i.e. no alternative route exists), the concerned traffic is restarted towards the signalling point from which the transfer-restricted message was received. Otherwise, no other actions are taken.

### 13.5 *Signalling-route-set-test*

13.5.1 The signalling-route-set-test procedure is used at a signalling point to test whether or not signalling traffic towards a certain destination may be routed via an adjacent signalling transfer point.

The procedure makes use of the signalling-route-set-test message, and the transfer-allowed and the transfer-prohibited procedures.

The signalling-route-set-test message contains:

- the label, indicating the destination and originating points;
- the signalling-route-set-test signal;
- the destination, the accessibility of which is to be tested; and
- the current route status of the destination being tested.[18)]

Format and coding of this message appear in § 15.

13.5.2 A signalling-route-set-test message is sent from a signalling point after a transfer-prohibited or transfer-restricted[19)] message is received from an adjacent signalling transfer point. In this case, a signalling-route-set-test message is sent to that signalling transfer point referring to the destination declared inaccessible or restricted by the transfer-prohibited or transfer-restricted[19)] message, every T10 period (see § 16) until a transfer-allowed message, indicating that the destination has become accessible, is received.

This procedure is used in order to recover the signalling route availability information that may not have been received because of some signalling network failure.

13.5.3 A signalling-route-set-test message is sent to the adjacent signalling transfer point as an ordinary signalling network management message.

13.5.4 At the reception of a signalling-route-set-test message, a signalling transfer point will compare the status of the destination in the received message with the actual status of the destination. If they are the same, no further action is taken. If they are different, one of the following messages is sent in response, dictated by the actual status of the destination:

- a transfer-allowed message, referring to the destination the accessibility of which is tested, if the signalling transfer point can reach the indicated destination via a signalling link not connected to the signalling point from which the signalling-route-set-test message was originated, and via the normal routing;
- a transfer-restricted[19)] message when access to the destination is possible via an alternative to the normal routing which is less efficient, but still not via the signalling point from which the signalling route-set-test was originated;
- a transfer-prohibited message in all other cases (including the inaccessibility of that destination).

---

[18)] The possibility of referring to a more general destination than a single signalling point (e.g. a signalling region), or a more restrictive destination than a single signalling point is for further study.

[19)] National option.

13.5.5 At the reception of the transfer-prohibited or transfer-allowed message, the signalling point will perform the procedures specified in §§ 13.2.3 or 13.2.4 and 13.3.3 or 13.3.4 respectively.

13.6 *Transfer controlled (International network)*

The only use made of the transfer controlled procedure in the international signalling network is to convey the congestion indication from the SP where congestion was detected to the originating SP (see § 11.2.3) in a transfer-controlled message.

The transfer-controlled message contains:

- the label, indicating the destination and originating points;
- the transfer controlled signal;
- the identity of the congested destination.

The format and coding of the transfer controlled message appear in § 15.

13.7 *Transfer controlled (National option with congestion priorities)*

13.7.1 The transfer-controlled procedure is performed at a signalling transfer point for messages relating to a given destination, when it has to notify one or more originating signalling points that they should no longer send to the concerned destination messages with a given priority or lower.

The transfer-controlled procedure makes use of the transfer-controlled message which contains:

- the label, indicating the destination and originating points,
- the transfer-controlled signal,
- the destination for which messages with a congestion priority lower than the specified congestion status should no longer be sent, and
- the current congestion status encountered in routing a particular message towards the concerned destination.

The format and coding of this message appear in § 15.

13.7.2 A transfer-controlled message relating to a given destination "X" is sent from a signalling transfer point "Y" in response to a received message originating from signalling point "Z" destined to signalling point "X" when the congestion priority of the concerned message is less than the current congestion status of the signalling link selected to transmit the concerned message from "Y" to "X".

In this case, the transfer-controlled message is sent to the originating point "Z" with the congestion status field set to the current congestion status of the signalling link.

13.7.3 When the originating signalling points "Z" receive a transfer-controlled message relating to destination "X", if the current congestion status of the signalling route set towards destination "X" is less than the congestion status in the transfer-controlled message, it updates the congestion status of the signalling route set towards destination "X" with the value of the congestion status carried in the transfer-controlled message.

13.7.4 If within T15 (see § 16) after the receipt of the last transfer-controlled message relating to destination "X", signalling point "Z" receives another transfer-controlled message relating to the same destination, the following action is taken: If the value of the congestion status carried in the new transfer-controlled message is greater than the current value of the congestion status of the signalling route set towards destination "X", then the current value is updated by the new value.

13.7.5 If T15 (see § 16) expires after the last update of the signalling route set towards destination "X" by a transfer-controlled message relating to the same destination, the signalling-route-set-congestion-test procedure is invoked (see § 13.9).

13.7.6 In some circumstances it may happen that a signalling point receives a transfer-controlled message relating to a destination which is already inaccessible due to previous failures; in this case the transfer-controlled message is ignored.

13.8 *Transfer controlled (National option without congestion priorities)*

The only use made of the TFC procedure by the national signalling network, using multiple congestion states without congestion priorities, is to convey the congestion indication primitive from the SP where congestion was detected to the originating SP (see § 11.2.5) in a transfer-controlled message.

The transfer-controlled message contains:

- the label, indicating the destination and originating points;
- the transfer-controlled signal;
- the identity of the congested destination;
- the current congestion status encountered in routing a particular message towards the concerned destination.

The format and coding of this message appear in § 15.

13.9 *Signalling-route-set-congestion-test (National Option)*

13.9.1 The signalling-route-set-congestion-test procedure is used at an originating signalling point to update the congestion status associated with a route set towards a certain destination. The purpose is to test whether or not signalling messages destined towards that destination with a given congestion priority or higher may be sent.

In the case of a processor restart the congestion status of all signalling route sets will be initialized to the zero value. The response mechanism within the transfer-controlled procedure will correct signalling route sets whose congestion status does not have the zero value.

The procedure makes use of the signalling-route-set-congestion-test message, and the transfer-controlled procedure.

The signalling-route-set-congestion-test message contains:

- the label, indicating the destination and originating points, and
- the signalling-route-set-congestion-test signal.

The format and coding of this message appear in § 15.

13.9.2 The signalling-route-set-congestion-test message differs from other signalling network management messages in that it is not assigned the highest congestion priority. Instead, the congestion priority assigned to a signalling-route-set-congestion-test message to be sent to a given destination is equal to one less than the current congestion status associated with the signalling route set towards the destination.

13.9.3 If within T16 (see § 16), after sending a signalling-route-set-congestion-test message, a transfer-controlled message relating to the concerned destination is received, the signalling point updates the congestion status of the signalling route set towards the concerned destination with the value of the congestion status carried in the transfer-controlled message. Following this, the procedures specified in §§ 13.9.4 and 13.9.5 are performed.

If T16 (see § 16) expires after sending a signalling-route-set-congestion-test message without a transfer-controlled message relating to the concerned destination having been received, the signalling point changes the congestion status associated with the signalling route set towards the concerned destination to the next lower status.

13.9.4 Provided that the signalling route set towards destination "X" is not in the "unavailable" state, a signalling-route-set-congestion-test message is sent from an originating signalling point to destination "X" in the following cases:

i) When T15 (see § 16) expires after the last update of the congestion status of the signalling route set toward destination "X" by a transfer-controlled message relating to the same destination.

ii) When T16 (see § 16) expires after sending a signalling-route-set-congestion-test message to destination "X" without a transfer-controlled message relating to the same destination having been received. After the congestion status has been decremented by one, the test is repeated, unless the congestion status is zero.

13.9.5 At the reception of a signalling-route-set-congestion-test message, a signalling transfer point will route it as an ordinary message, i.e. according to the procedure specified in § 2.3.5.

13.9.6 When a signalling-route-set-congestion-test message reaches its destination, it is discarded.

## 14 Common characteristics of message signal unit formats

### 14.1 *General*

The basic signal unit format which is common to all message signal units is described in Recommendation Q.703, § 2. From the point of view of the Message Transfer Part level 3 functions, common characteristics of the message signal units are the presence of:

- the service information octet;
- the label, contained in the signalling information field, and, in particular, the routing label.

### 14.2 *Service information octet*

The service information octet of message signal units contains the service indicator and the sub-service field. The structure of the service information octet is shown in Figure 13/Q.704.

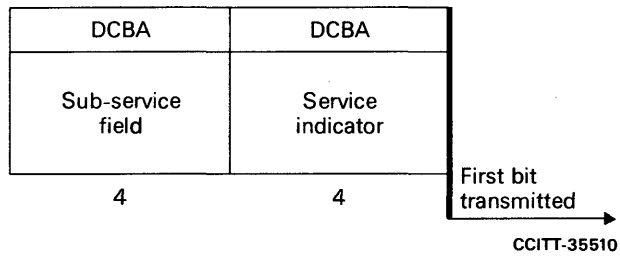



FIGURE 13/Q.704
**Service information octet**

#### 14.2.1 *Service indicator*

The service indicator is used by signalling handling functions to perform message distribution (see § 2.4) and, in some special applications, to perform message routing (see § 2.3).

The service indicator codes *for the international signalling network* are allocated as follows:

| bits D C B A | |
|---|---|
| 0 0 0 0 | Signalling network management messages |
| 0 0 0 1 | Signalling network testing and maintenance messages |
| 0 0 1 0 | Spare |
| 0 0 1 1 | SCCP |
| 0 1 0 0 | Telephone User Part |
| 0 1 0 1 | ISDN User Part |
| 0 1 1 0 | Data User Part (call and circuit related messages) |
| 0 1 1 1 | Data User Part (facility registration and cancellation messages) |
| 1 0 0 0 | Reserved for MTP Testing User Part |
| 1 0 0 1 | spare |
| 1 0 1 0 | |
| 1 0 1 1 | |
| 1 1 0 0 | |
| 1 1 0 1 | |
| 1 1 1 0 | |
| 1 1 1 1 | |

The allocation of the service indicator codes for national signalling networks is a national matter. However, it is suggested to allocate the same service indicator code to a User Part which performs similar functions as in the international network.

14.2.2 *Sub-service field*

The sub-service field contains the network indicator (bits C and D) and two spare bits (bits A and B).

The *network* indicator is used by signalling message handling functions (e.g., in order to determine the relevant version of a User Part), see §§ 2.3 and 2.4.

If the network indicator is set to 00 or 01, the two spare bits, coded 00, are available for possible future needs that may require a common solution for all international User Parts.

If the network indicator is set to 10 or 11, the two spare bits are for national use. They may be used, for example, to indicate message priority, which is used in the optional flow control procedure in national applications.

The network indicator provides for discrimination between international and national messages. It can also be used, for example, for the discrimination between functionally two national signalling networks, each having different routing label structures and including up to 16 User Parts defined by the 16 possible codes of the service indicator.

In the case of only one national signalling network the spare code of the network indicator reserved for national use can be used, for example, to define an additional 16 User Parts (making a total of 32 User Parts) for that national signalling network.

The network indicator codes are allocated as follows:

| bits D | C | |
|---|---|---|
| 0 | 0 | International network |
| 0 | 1 | Spare (for international use only) |
| 1 | 0 | National network |
| 1 | 1 | Reserved for national use |

The international spare code (01) should not be used for implementing features which are to be provided both internationally and nationally.

In national applications, when the discrimination provided by the network indicator between international and national messages is not used, i.e. in a closed national signalling network seen from the signalling point of view, the whole sub-service field can be used independently for different User Parts.

14.3 *Label*

The structure and content of the label is defined for each User Part and is defined in the relevant specification. The common part of the label used for signalling message handling, the routing label, is specified in § 2.2.

## 15 Formats and codes of signalling network management messages

15.1 *General*

15.1.1 The signalling network management messages are carried on the signalling channel in message signal units, the format of which is described in § 14 and in Recommendation Q.703, § 2. In particular, as indicated in § 14.2 these messages are distinguished by the configuration 0000 of the service indicator (SI). The sub-service field (SSF) of the messages is used according to the rules indicated in § 14.2.2.

15.1.2 The signalling information field consists of an integral number of octets and contains the label, the heading code and one or more signals and indications. The structure and function of the label, and of the heading code, are described in §§ 15.2 and 15.3 respectively; the detailed message formats are described in the following sections. For each message the sequence of fields is shown in the corresponding figure, including fields that may or may not be present.

In the figures, the fields are shown starting from the right to the left (i.e. the first field to be transmitted is at the right). Within each field the information is transmitted least significant bit first. Spare bits are coded 0 unlesss otherwise indicated.

15.2 *Label*

For signalling network management messages the label coincides with the routing label and indicates the destination and originating signalling points of the message; moreover, in the case of messages related to a particular signalling link, it also indicates the identity of the signalling link among those interconnecting the destination and originating points. The standard label structure of Message Transfer Part level 3 messages appears in Figure 14/Q.704; the total length is 32 bits.

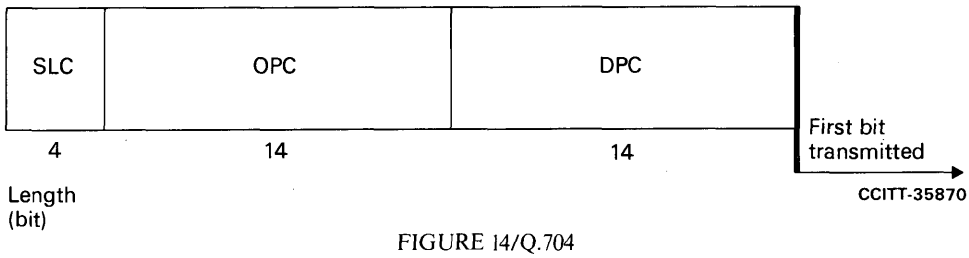



FIGURE 14/Q.704
**Standard label structure**

The meaning and use of the destination point code (DPC) and of the originating point code (OPC) fields are described in § 2. The signalling link code (SLC) indicates the signalling link, connecting the destination and originating points, to which the message is related. If the message is not related to a signalling link, or another particular code is not specified, it is coded 0000.

15.3 *Heading code (H0)*

The heading code (H0) is the 4 bit field following the label and identifies the message group.

The different heading codes are allocated as follows:

0000 Spare
0001 Changeover and changeback messages
0010 Emergency changeover message
0011 Transfer controlled and signalling route set congestion messages
0100 Transfer-prohibited-allowed-restricted messages
0101 Signalling-route-set-test messages
0110 Management inhibit messages
0111 Traffic restart allowed message
1000 Signalling-data-link-connection messages
1001 Spare
1010 User part flow control messages

The remaining codings are spare.

The synopsis of singalling network management messages is given in Table 1/Q.704.

15.4 *Changeover message*

15.4.1 The format of the changeover message is shown in Figure 15/Q.704.

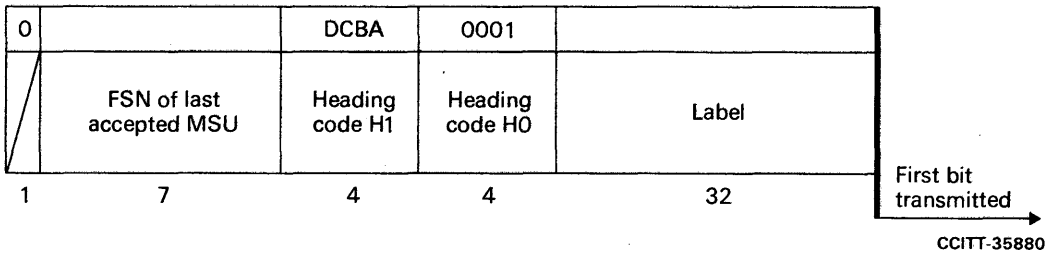



FIGURE 15/Q.704
**Changeover message**

15.4.2 The changeover message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.4.3
- Forward sequence number of last accepted message signal unit (7 bits)
- A filler bit coded 0

15.4.3 The heading code H1 contains signal codes as follows:

bit D C B A

0 0 0 1 Changeover order signal

0 0 1 0 Changeover acknowledgement signal

15.5 *Changeback message*

15.5.1 The format of the changeback message is shown in Figure 16/Q.704.

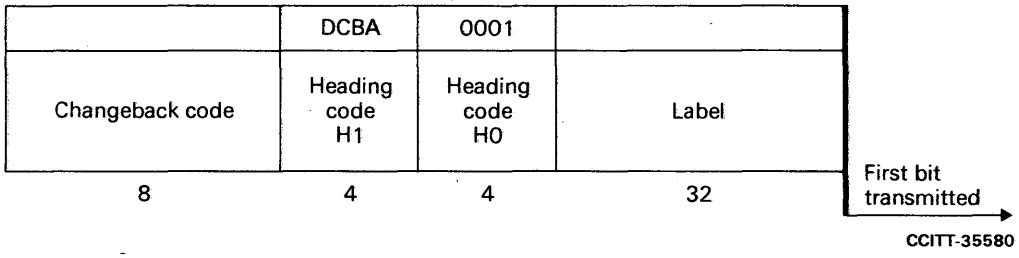



FIGURE 16/Q.704
**Changeback message**

15.5.2 The changeback message is made up of the following fields:

- Label (32 bits) see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.5.3
- Changeback code (8 bits): see § 15.5.4

15.5.3 The header code H1 contains signal codes as follows:

bit D C B A

0 1 0 1 Changeback declaration signal

0 1 1 0 Changeback acknowledgement signal

15.5.4 The changeback code is an 8 bit code assigned by the signalling point which sends the message according to the criteria described in § 6.

15.6 *Emergency changeover message*

15.6.1 The format of the emergency changeover message is shown in Figure 17/Q.704.

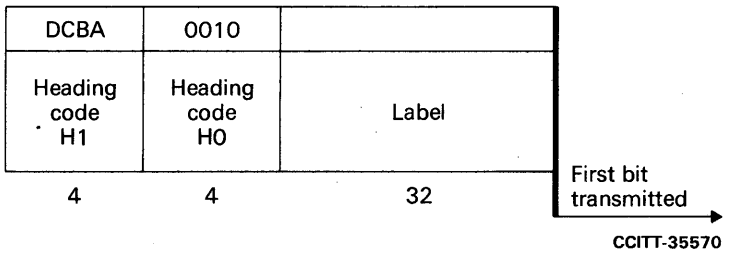



FIGURE 17/Q.704

**Emergency changeover message**

15.6.2 The emergency changeover message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.6.3

15.6.3 The header code H1 contains signal codes as follows:

bit D C B A

0 0 0 1 Emergency changeover order signal

0 0 1 0 Emergency changeover acknowledgement signal

15.7 *Transfer-prohibited message*

15.7.1 The format of the transfer-prohibited message is shown in Figure 18/Q.704.

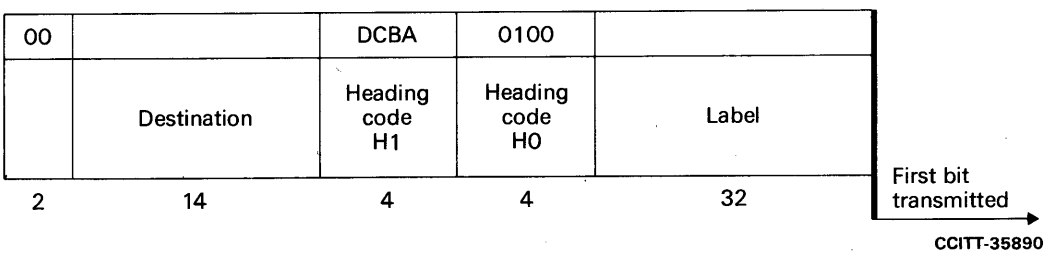



FIGURE 18/Q.704

**Transfer-prohibited message**

15.7.2 The transfer-prohibited message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.7.3
- Destination (14 bits): see § 15.7.4
- Spare bits (2 bits) code 00

15.7.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 0 0 1 Transfer-prohibited signal

15.7.4 The destination field contains the identity of the signalling point to which the message refers.

15.8 *Transfer-allowed message*

15.8.1 The format of the transfer-allowed message is shown in Figure 19/Q.704.

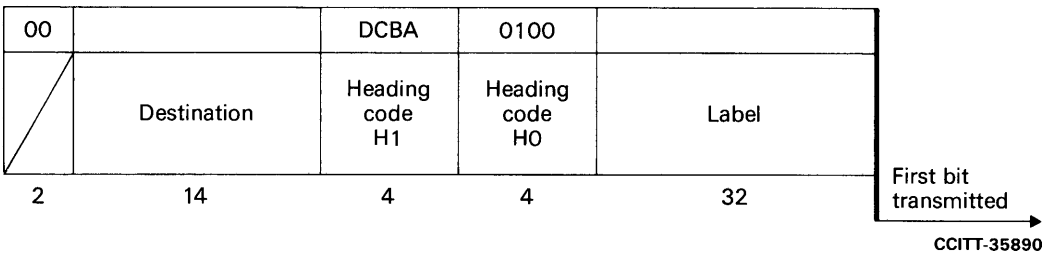



FIGURE 19/Q.704

**Transfer-allowed message**

15.8.2 The transfer-allowed message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.8.3
- Destination (14 bits): see § 15.7.4
- Spare bits (2 bits) coded 00

*Note* – For the use of the 2 spare bits in the national option for a SIF compatibility mechanism, see Recommendation Q.701, § 7.2.6.

15.8.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 1 0 1 Transfer-allowed signal

15.9 *Transfer restricted message (national option)*

15.9.1 The format of the transfer restricted message is shown in Figure 18/Q.704.

15.9.2 The transfer restricted message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.9.3
- Destination (14 bits): see § 15.9.4
- Spare (2 bits) coded 00

15.9.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 0 1 1 Transfer restricted

15.9.4 The destination field contains the identity of the signalling point to which the message refers.

15.10 *Signalling-route-set-test message*

15.10.1 The format of the signalling-route-set-test message is shown in Figure 20/Q.704.

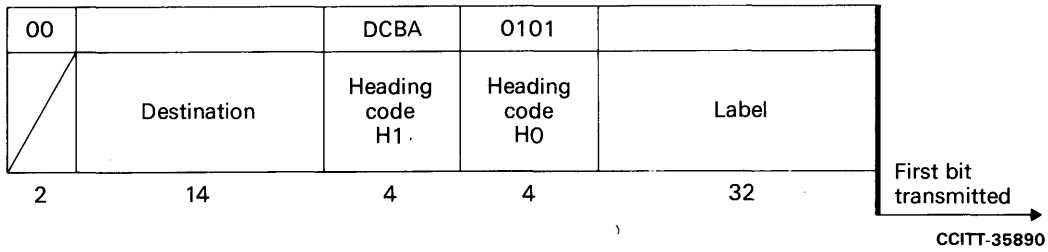



FIGURE 20/Q.704

**Signalling-route-set-test message**

15.10.2 This message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.10.3
- Destination (14 bits): see § 15.7.4
- Spare bits (2 bits) coded 00

15.10.3 The heading code H1 contains signal codes as follows:

bit D C B A

0 0 0 1 Signalling-route-set-test signal for prohibited destination

0 0 1 0 Signalling-route-set-test signal for restricted destination (national option)

15.11 *Management inhibit message*

15.11.1 The format of the management inhibit message is shown in Figure 20a/Q.704.

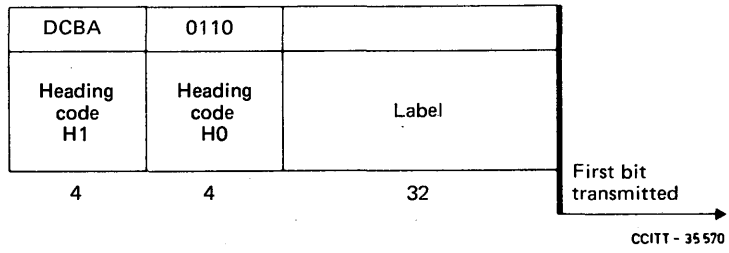



FIGURE 20a/Q.704

**Management inhibit message**

15.11.2 The management inhibit message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.11.3

15.11.3 The header code H1 contains signal codes as follows:

bit D C B A

0 0 0 1 Link inhibit signal
0 0 1 0 Link uninhibit signal
0 0 1 1 Link inhibited acknowledgement signal
0 1 0 0 Link uninhibited acknowledgement signal
0 1 0 1 Link inhibit denied signal
0 1 1 0 Link force uninhibit signal
0 1 1 1 Link local inhibit test signal
1 0 0 0 Link remote inhibit test signal

15.12 *Traffic restart allowed message*

15.12.1 The format of the traffic restart allowed message is shown in Figure 21/Q.704.

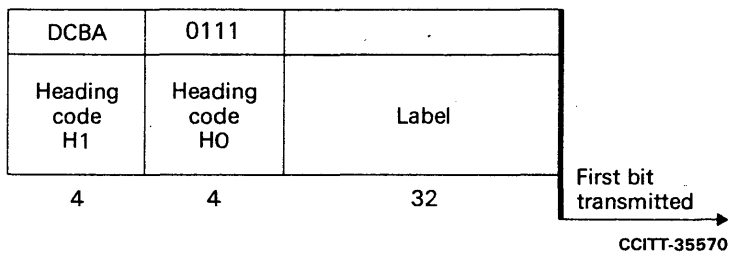



FIGURE 21/Q.704

**Traffic restart allowed message**

15.12.2 The traffic restart allowed message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.12.3

15.12.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 0 0 1 Traffic restart allowed signal

15.13 *Signalling-data-link-connection-order message*

15.13.1 The format of the signalling-data-link-connection-order message is shown in Figure 22/Q.704.

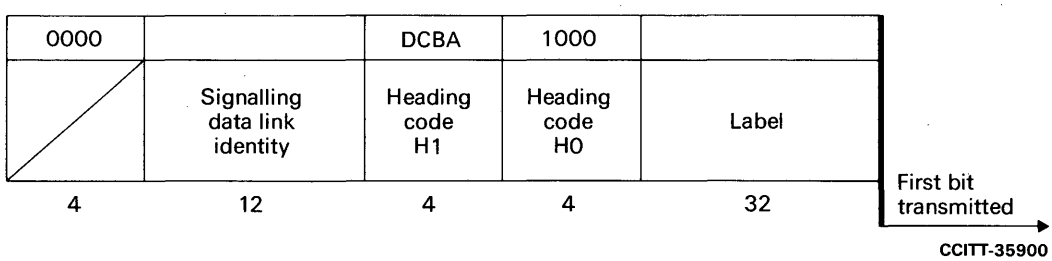



FIGURE 22/Q.704

**Signalling-data-link-connection-order message**

15.13.2 The signalling-data-link-connection-order message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.13.3
- Signalling data link identity (12 bits): see § 15.13.4
- Spare bits (4 bits) coded 0000.

15.13.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 0 0 1 Signalling-data-link-connection-order signal

15.13.4 The signalling data link identity field contains the circuit identification code (CIC), or the bearer identification code (BIC) in case of a 64 kbit/s channel used to carry submultiplex data streams, of the transmission link corresponding to the signalling data link.

15.14 *Signalling-data-link-connection-acknowledgement message*

15.14.1 The format of the signalling-data-link-connection-acknowledgement message is shown in Figure-22a/Q.704.

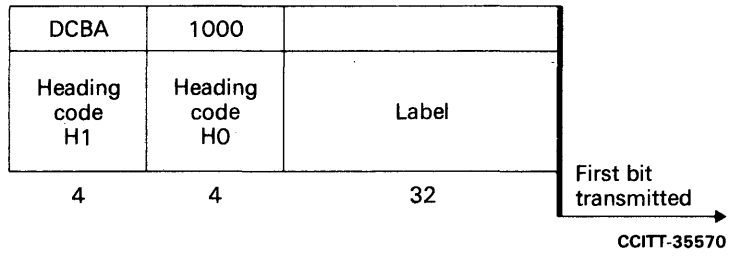



FIGURE 22a/Q.704

**Signalling-data-link-connection-acknowledgement message**

15.14.2 The signalling-data-link-connection acknowledgement message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.14.3

15.14.3 The heading code H1 contains signal codes as follows:

bit D C B A

0 0 1 0 Connection-successful signal

0 0 1 1 Connection-not-successful signal

0 1 0 0 Connection-not-possible signal

15.15 *Transfer controlled message*

15.15.1 The format of the TFC message is shown in Figure 22b/Q.704.

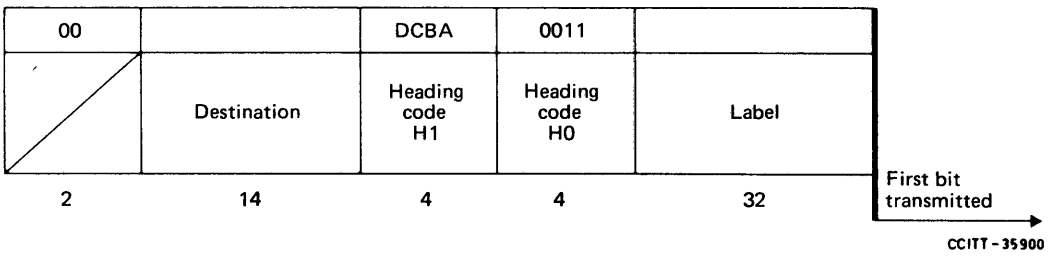



FIGURE 22b/Q.704

**Transfer controlled message**

15.15.2 The transfer controlled message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.15.3
- Destination (14 bits): see § 15.15.4
- Spare (2 bits): see §15.15.5

15.15.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 0 1 0 Transfer controlled signal

15.15.4 The destination field carries the address of the destination to which the message refers.

15.15.5 In national signalling networks using multiple congestion states, the spare bits in the transfer controlled message are used to carry the congestion status associated with the destination.

15.16 *Signalling-route-set-congestion-test message (national option)*

15.16.1 The format of the signalling-route-set-congestion-test message is shown in Figure 22c/Q.704.

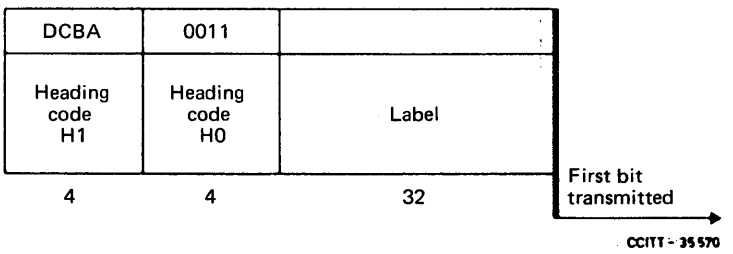



FIGURE 22c/Q.704

**Signalling-route-set-congestion-test message**

15.16.2 The signalling-route-set-congestion test message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.16.3

15.16.3 The heading code H1 contains one signal code as follows:

bit D C B A

0 0 0 1 Signalling-route-set-congestion-test signal

15.17 *User part unavailable message*

15.17.1 The format of the user part unavailable message is shown in Figure 22d/Q.704.

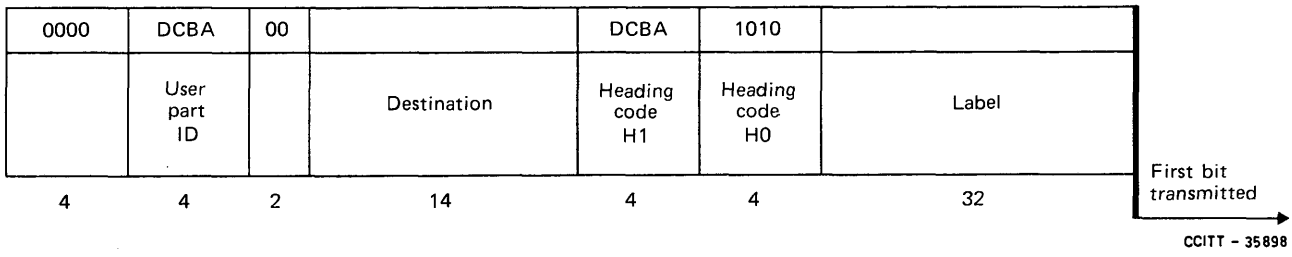



FIGURE 22d/Q.704

**User part unavailable message**

15.17.2 The user part unavailable message is made up of the following fields:

- Label (32 bits): see § 15.2
- Heading code H0 (4 bits): see § 15.3
- Heading code H1 (4 bits): see § 15.17.3
- Destination (14 bits): see § 15.15.4
- Spare (2 bits): coded 00
- User part identity (4 bits): see § 15.17.4
- Spare (4 bits) coded 0000

15.17.3 The heading code H1 contains signal codes as follows:

bit D C B A

0 0 0 1 User part unavailable

15.17.4 The user part identity is coded as follows:

bit D C B A

0 0 0 0 Spare
0 0 0 1 Spare
0 0 1 0 Spare
0 0 1 1 SCCP
0 1 0 0 TUP
0 1 0 1 ISUP
0 1 1 0 DUP
0 1 1 1 Spare
1 0 0 0 MTP Testing User Part
1 0 0 1 to 1 1 1 1 Spare

TABLE 1/Q.704

**Heading code allocation of signalling network management messages**

| Message Group | H1 / H0 | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0000 | | | | | | | | | | | | | | | | |
| CHM | 0001 | | COO | COA | | | CBD | CBA | | | | | | | | | |
| ECM | 0010 | | ECO | ECA | | | | | | | | | | | | | |
| FCM | 0011 | | RCT | TFC | | | | | | | | | | | | | |
| TFM | 0100 | | TFP | * | TFR | | TFA | * | | | | | | | | | |
| RSM | 0101 | | RST | RSR | | | | | | | | | | | | | |
| MIM | 0110 | | LIN | LUN | LIA | LUA | LID | LFU | LLT | LRT | | | | | | | |
| TRM | 0111 | | TRA | | | | | | | | | | | | | | |
| DLM | 1000 | | DLC | CSS | CNS | CNP | | | | | | | | | | | |
| | 1001 | | | | | | | | | | | | | | | | |
| UFC | 1010 | | UPU | | | | | | | | | | | | | | |
| | 1011 | | | | | | | | | | | | | | | | |
| | 1100 | | | | | | | | | | | | | | | | |
| | 1101 | | | | | | | | | | | | | | | | |
| | 1110 | | | | | | | | | | | | | | | | |
| | 1111 | | | | | | | | | | | | | | | | |

*Note* – Values marked * should not be used (codes used in the Yellow Book for TFP and TFA acknowledgement).

CBA Changeback-acknowledgement signal

CBD Changeback-declaration signal

CHM Changeover and changeback messages

CNP Connection-not-possible signal

CNS Connection-not-successful signal

COA Changeover-acknowledgement signal

COO Changeover-order signal

CSS Connection-successful signal

DLC Signalling-data-link-connection-order signal

DLM Signalling-data-link-connection-order message

ECA Emergency-changeover-acknowledgement signal

ECM Emergency-changeover message

ECO Emergency-changeover-order signal

FCM Signalling-traffic-flow-control messages

RCT Signalling-route-set-congestion-test signal

RSM Signalling-route-set-test message

RSR Signalling-route-set-test signal for restricted destination (national option)

RST Signalling-route-set-test signal for prohibited destination

TFR Transfer-restricted signal (national option)

TFA Transfer-allowed signal

TFC Transfer-controlled signal

TFM Transfer-prohibited-transfer-allowed-transfer-restricted messages

TFP Transfer-prohibited signal

TRA Traffic-restart-allowed signal

TRM Traffic-restart-allowed message

MIM Management inhibit messages

LID Link inhibit denied signal

LFU Link forced uninhibit signal

LIN Link inhibit signal

LIA Link inhibit acknowledgement signal

LUA Link uninhibit acknowledgement signal

LUN Link uninhibit signal

LLT Link local inhibit test signal

LRT Link remote inhibit test signal

UFC User part flow control messages

UPU User part unavailable signal

## 16 State transition diagrams

### 16.1 *General*

§ 16 contains the description of the signalling network functions described in §§ 2 to 13 in the form of state transition diagrams according to the CCITT Specification and Description Language (SDL).

A set of diagrams is provided for each of the following major functions:

- signalling message handling (SMH), described in § 2;
- signalling traffic management (STM), described in §§ 4 to 11;
- signalling route management (SRM), described in § 13;
- signalling link management (SLM), described in § 12.

16.1.1 For each major function a figure illustrates a subdivision into functional specification blocks, showing their functional interactions as well as the interactions with the other major functions. In each case this is followed by figures showing state transition diagrams for each of the functional specification blocks.

The detailed functional breakdown shown in the following diagrams is intended to illustrate a reference model and to assist interpretation of the text in the earlier sections. The state transition diagrams are intended to show precisely the behaviour of the signalling system under normal and abnormal conditions as viewed from a remote location. It must be emphasized that the functional partitioning shown in the following diagrams is used only to facilitate understanding of the system behaviour and is not intended to specify the functional partitioning to be adopted in a practical implementation of the signalling system.

16.2 *Drafting conventions*

16.2.1 Each major function is designated by its acronym (e.g. SMH = signalling message handling).

16.2.2 Each functional block is designated by an acronym which identifies it and also identifies the major function to which it belongs (e.g. HMRT = signalling message handling-message routing; TLAC = signalling traffic management-link availability control).

16.2.3 External inputs and outputs are used for interactions between different functional blocks. Included within each input and output symbol in the state transition diagrams are acronyms which identify the functions which are the source and destination of the message, e.g.:

L2 → L3 indicates that the message is sent between functional levels:

from: functional level 2,
to: functional level 3.

RTPC → TSRC indicates that the message is sent within a functional level (3 in this case):

from: signalling route management-transfer prohibited control,
to: signalling traffic management-signalling routing control.

16.2.4 Internal inputs and outputs are only used to indicate control of time-outs.

16.2.5 *Notations for national operations*

National options are included in the main body of the state transition diagrams (STDs) with dotted or dashed lines; if their use should exclude or modify some of the international logic, the relevant sections are marked "t" and a note is added to the figure. Also, the options are marked as follows:

Transfer restricted – dashed lines.

Multiple congestion states – dotted lines (with the hatched symbols removed where shown).

16.3 *Signalling message handling*

Figure 23/Q.704 shows a subdivision of the signalling message handling (SMH) function into smaller functional specification blocks and also shows the functional interactions between them. Each of these functional specification blocks is described in detail in a state transition diagram as follows:

a) message discrimination (HMDC) is shown in Figure 24/Q.704;
b) message distribution (HMDT) is shown in Figure 25/Q.704;
c) message routing (HMRT) is shown in Figure 26/Q.704;
d) handling of messages under signalling link congestion is shown in Figure 26a/Q.704.

16.4 *Signalling traffic management*

Figure 27/Q.704 shows a subdivision of the signalling traffic management (STM) function into smaller functional specification blocks and also shows functional interactions between them. Each of these functional specification blocks is described in detail in a state transition diagram as follows:

a) link availability control (TLAC) is shown in Figure 28/Q.704;
b) signalling routing control (TSRC) is shown in Figure 29/Q.704;
c) changeover control (TCOC) is shown in Figure 30/Q.704;
d) changeback control (TCBC) is shown in Figure 31/Q.704;
e) forced rerouting control (TFRC) is shown in Figure 32/Q.704;
f) controlled rerouting control (TCRC) is shown in Figure 33/Q.704;
g) signalling traffic flow control (TSFC) is shown in Figure 34a/Q.704;
h) signalling route set congestion control (TRCC) is shown in Figure 29a/Q.704;
i) signalling point restart control (TPRC) is shown in Figure 34b/Q.704.

16.5 *Signalling link management*

Figure 35/Q.704 shows a subdivision of the signalling link management function (SLM) into smaller functional specification blocks and also shows functional interactions between them. Each of these functional specification blocks is described in detail in a state transition diagram as follows:

a) link set control (LLSC) is shown in Figure 36/Q.704;

b) signalling link activity control (LSAC) is shown in Figure 37/Q.704;

c) signalling link activation (LSLA) is shown in Figure 38/Q.704;

d) signalling link restoration (LSLR) is shown in Figure 39/Q.704;

e) signalling link deactivation (LSLD) is shown in Figure 40/Q.704;

f) signalling terminal allocation (LSTA) is shown in Figure 41/Q.704;

g) signalling data link allocation (LSDA) is shown in Figure 42/Q.704.

16.6 *Signalling route management*

Figure 43/Q.704 shows a subdivision of the signalling route management (SRM) function into smaller functional specification blocks and also shows functional interactions between them. Each of these functional specification blocks is described in detail in a state transition diagram as follows:

a) transfer prohibited control (RTPC) is shown in Figure 44/Q.704;

b) transfer allowed control (RTAC) is shown in Figure 45/Q.704;

c) transfer restricted control (RTRC) is shown in Figure 46c/Q.704;

d) transfer controlled control (RTCC) is shown in Figure 46a/Q.704;

e) signalling route set test control (RSRT) is shown in Figure 46/Q.704;

f) signalling-route-set-congestion-test control (RCAT) is shown in Figure 46b/Q.704.

16.7 *Abbreviations used in Figures 23/Q.704 onwards*

BSNT Backward sequence number of next signal unit to be transmitted

DPC Destination point code

FSNC Forward sequence number of last message signal unit accepted by remote level 2

HMCG Signalling link congestion

HMDC Message discrimination

HMDT Message distribution

HMRT Message routing

L1 Level 1

L2 Level 2

L3 Level 3

L4 Level 4

LLSC Link set control

LSAC Signalling link activity control

LSDA Signalling data link allocation

LSLA Signalling link activation

LSLD Signalling link deactivation

LSLR Signalling link restoration

LSTA Signalling terminal allocation

MGMT Management system

RCAT Signalling-route-set-congestion-test control

RSRT Signalling route set test control

RTAC Transfer allowed control

RTCC Transfer controlled control

RTPC Transfer prohibited control

RTRC Transfer restricted control

SLM Signalling link management

SLS Signalling link selection

SLTC Signalling link test control

SMH Signalling message handling

SRM Signalling route management

STM Signalling traffic management

TCBC Changeback control

TCOC Changeover control

TCRC Controlled rerouting control

TFRC Forced rerouting control

TLAC Link availability control

TPRC Signalling point restart control

TRCC Signalling route set congestion control

TSFC Signalling traffic flow control

TSRC Signalling routing control

16.8 *Timers and timer values*

The following timers have been defined. The ranges are given below. The values, in brackets, are the minimum values for use when routes with long propagation delays are used (e.g., routes including satellite sections).

T1 Delay to avoid message mis-sequencing on changeover.
500 (800) to 1200 ms.

T2 Waiting for changeover acknowledgement.
700 (1400) to 2000 ms.

T3 Time controlled diversion-delay to avoid mis-sequencing on changeback.
500 (800) to 1200 ms.

T4 Waiting for changeback acknowledgement (first attempt).
500 (800) to 1200 ms.

T5 Waiting for changeback acknowledgement (second attempt).
500 (800) to 1200 ms.

T6 Delay to avoid message mis-sequencing on controlled rerouting.
500 (800) to 1200 ms.

T7 Waiting for signalling data link connection acknowledgement.
1 to 2 seconds.

T8 Transfer prohibited inhibition timer (transient solution).
800 to 1200 ms.

T9 Not used.

T10 Waiting to repeat signalling route set test message.
30 to 60 seconds.

T11 Transfer restricted timer. (This is one way of implementing the function described in § 13.4 and mainly intended to simplify STPs.)
30 to 90 seconds.

T12 Waiting for uninhibit acknowledgement.
800 to 1500 ms.

T13 Waiting for force uninhibit.
800 to 1500 ms.

T14 Waiting for inhibition acknowledgement.
2 to 3 seconds.

T15 Waiting to start signalling route set congestion test.
2 to 3 seconds.

T16 Waiting for route set congestion status update.
1.4 to 2 seconds.

T17 Delay to avoid oscillation of initial alignment failure and link restart.
800 to 1500 ms.

T18 Timer at restarting STP, waiting for signalling links to become available.
20 seconds (provisional value).

T19 Timer at restarting STP, started after T18, waiting to receive all traffic restart allowed messages.
4 seconds (provisional value).

T20 Timer at restarting STP, started after T19, waiting to broadcast traffic restart allowed messages, and restart remaining traffic.
4 seconds (provisional value).

T21 Timer at restarting signalling point having no STP function, waiting to restart traffic routed through adjacent SP;
AND timer at STP adjacent to restarting STP, waiting for traffic restart allowed message;
AND timer at SP having no STP function adjacent to restarting SP, waiting to restart any traffic to route through adjacent SP.
30 seconds (provisional value).

T22 Local inhibit test timer.
3 min to 6 min (provisional value).

T23 Remote inhibit test timer.
3 min to 6 min (provisional value).

T24 Stabilising timer after removal of local processor outage, used in LPO latching to RPO (national option).
500 ms (provisional value).

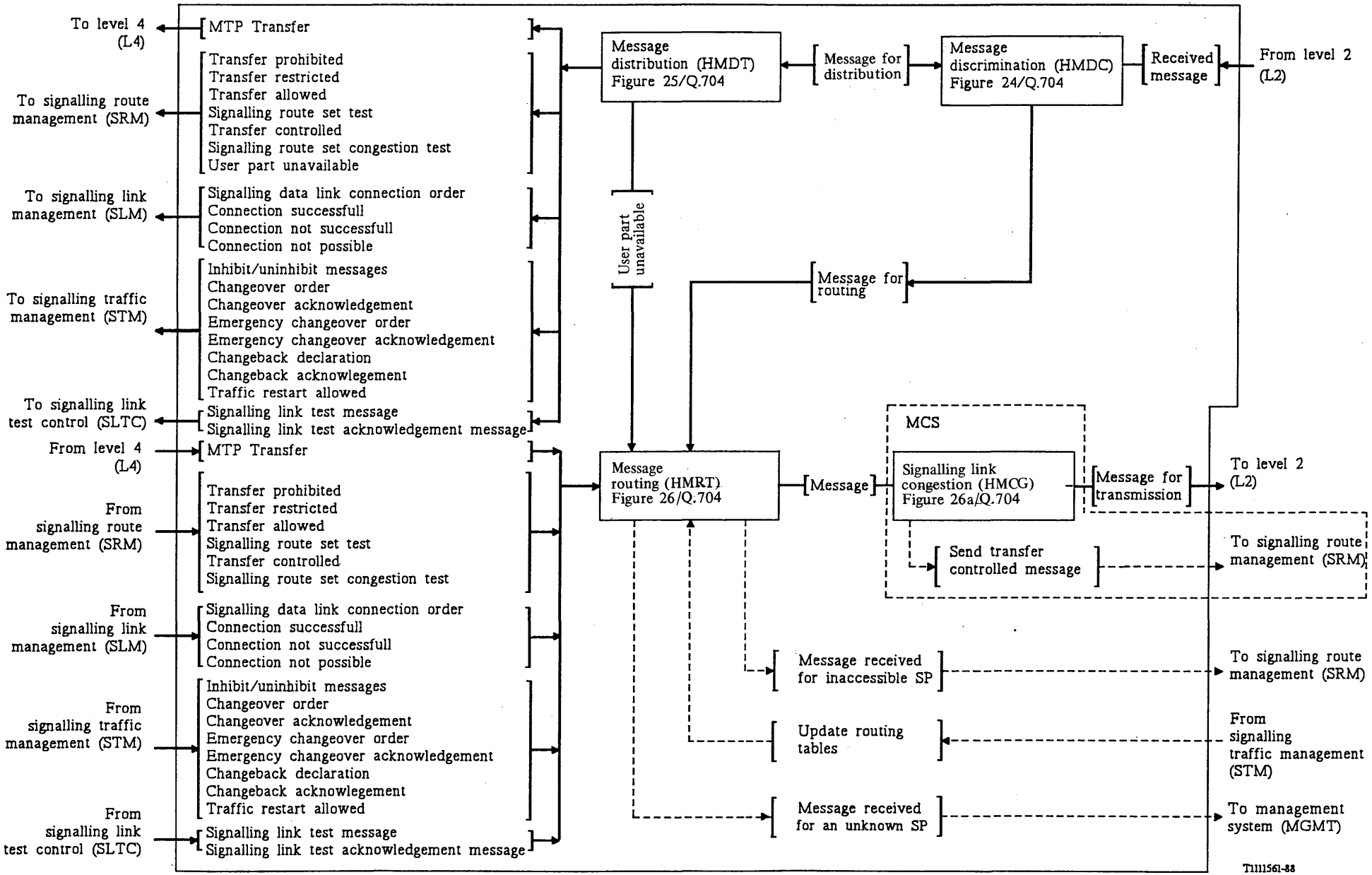



FIGURE 23/Q.704

**Level 3 - Signalling message handling (SMH); functional block interactions**

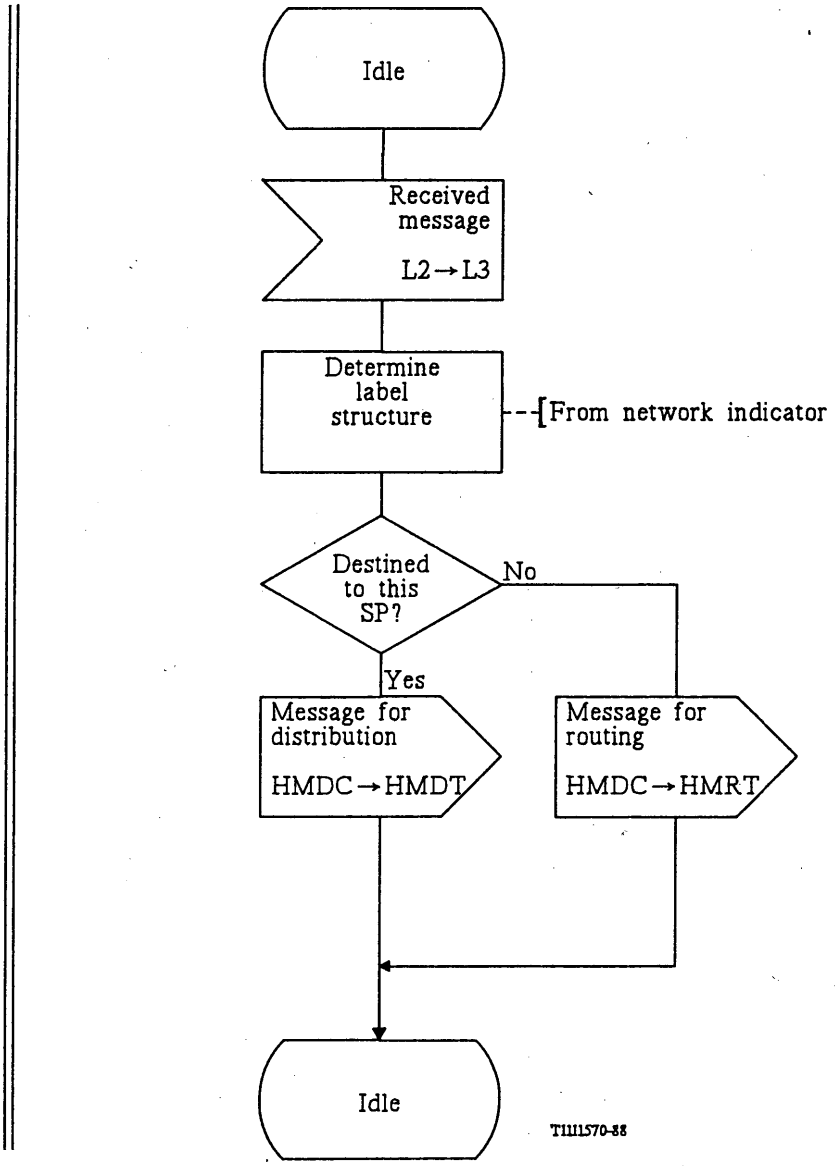
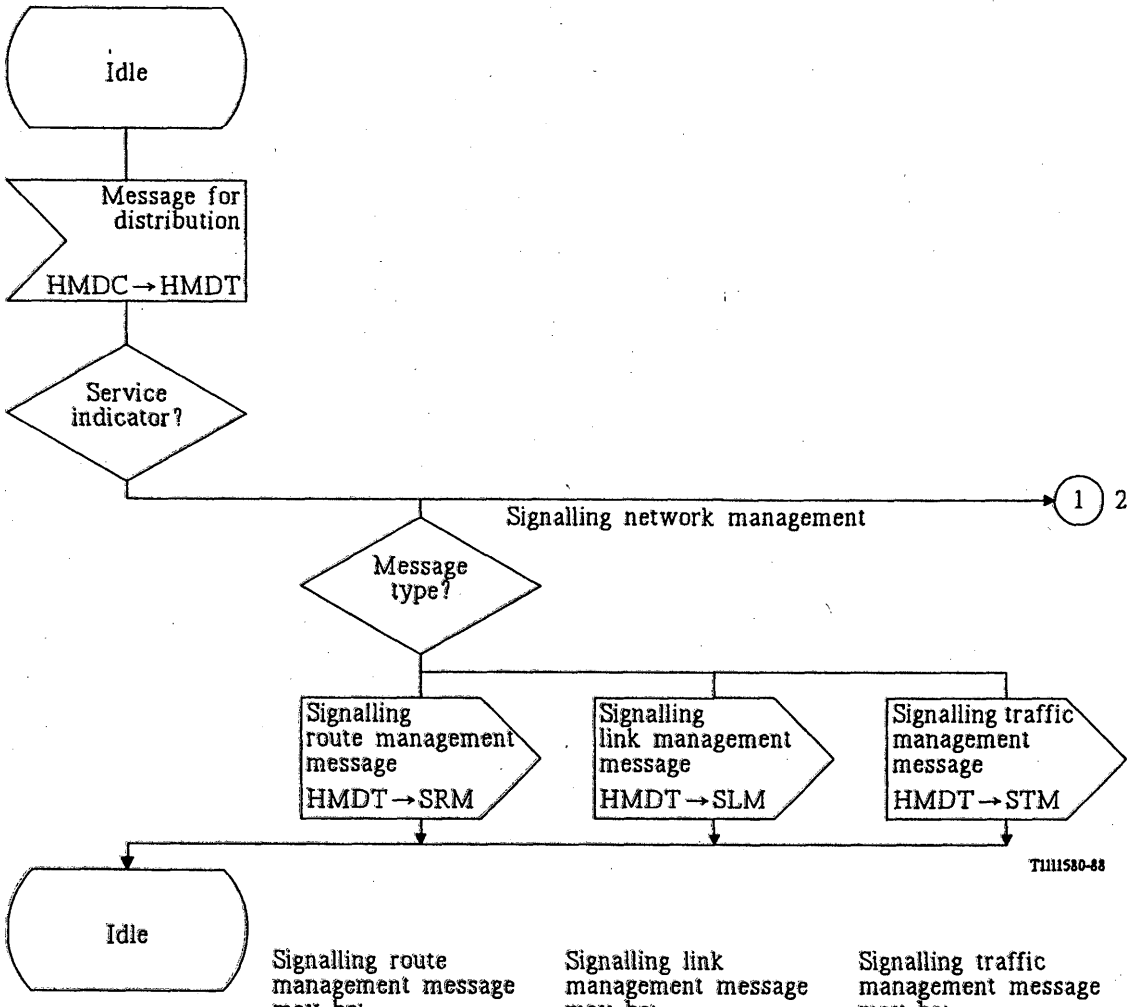



FIGURE 24/Q.704

Signalling message handling; message discrimination (HMDC)




Signalling route management message may be:

- transfer prohibited;
- transfer restricted;
- signalling route set test;
- transfer allowed;
- transfer controlled;
- signalling route set congestion test;
- user part unavailable.

Signalling link management message may be:

- signalling data link connection order;
- connection successful;
- connection not successful;
- connection not possible.

Signalling traffic management message may be:

- changeover acknowledgement;
- emergency changeover acknowledgement;
- changeback declaration;
- changeback acknowledgement;
- changeover order;
- emergency changeover order;
- inhibit signalling link;
- uninhibit signalling link;
- inhibit acknowledgement;
- uninhibit acknowledgement;
- inhibit denied;
- force uninhibit signalling link;
- traffic restart allowed.
- remote inhibit test;
- local inhibit test;

FIGURE 25/Q.704 (Sheet 1 of 2)

**Signalling message handling; message distribution (HMDT)**

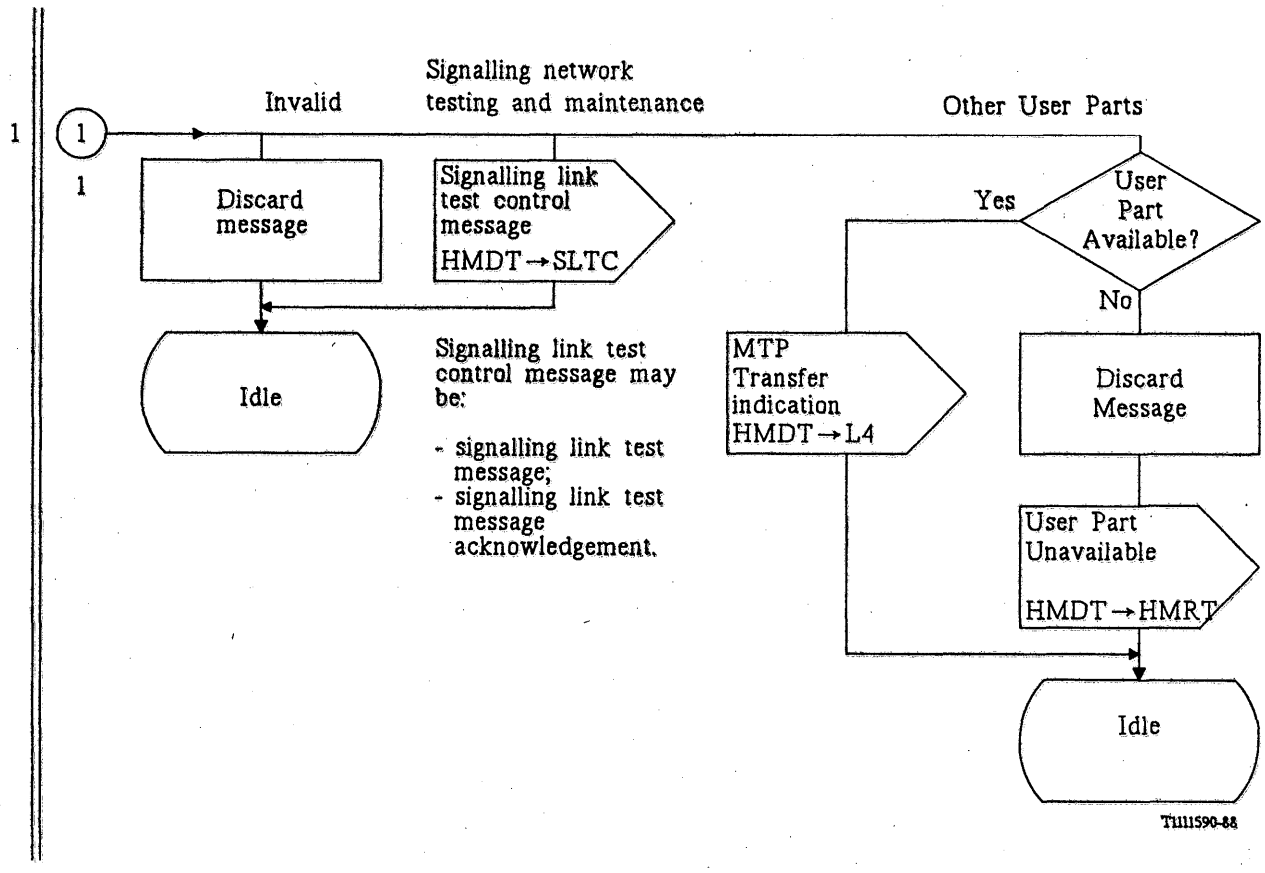
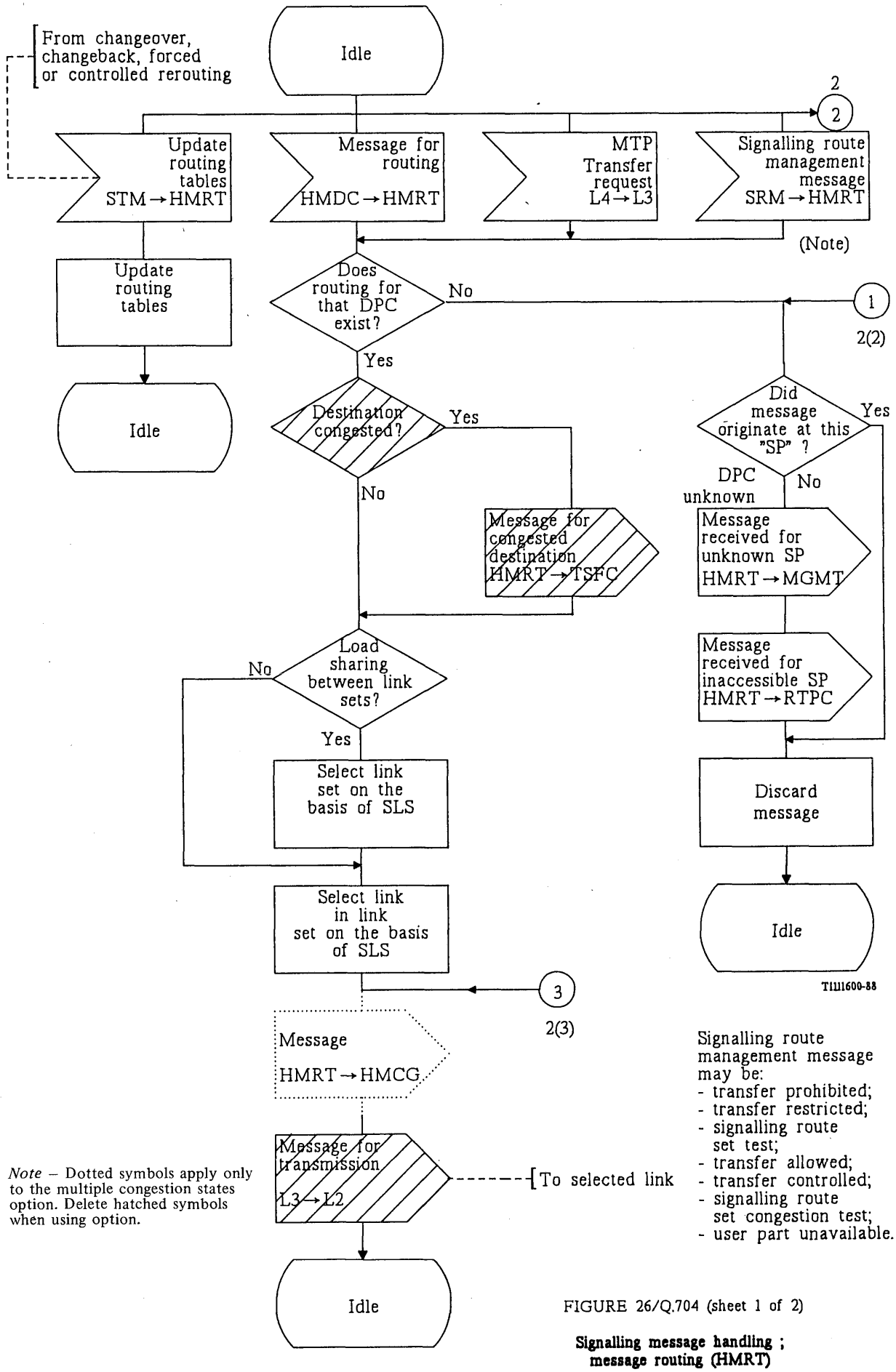



FIGURE 25/Q.704 (Sheet 2 of 2)

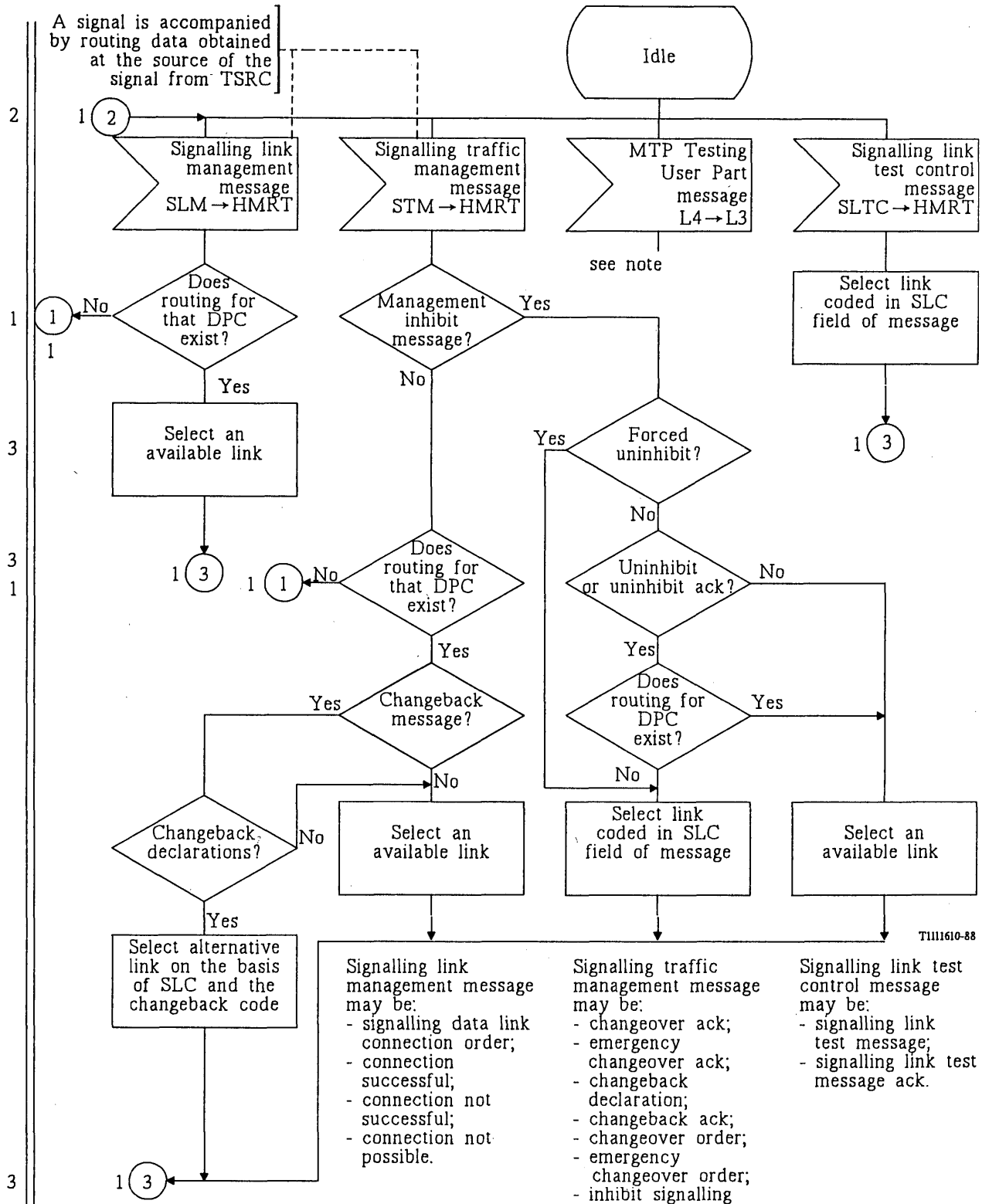
**Signalling message handling; message distribution (HMDT)**




*Note* – Dotted symbols apply only to the multiple congestion states option. Delete hatched symbols when using option.

FIGURE 26/Q.704 (sheet 1 of 2)

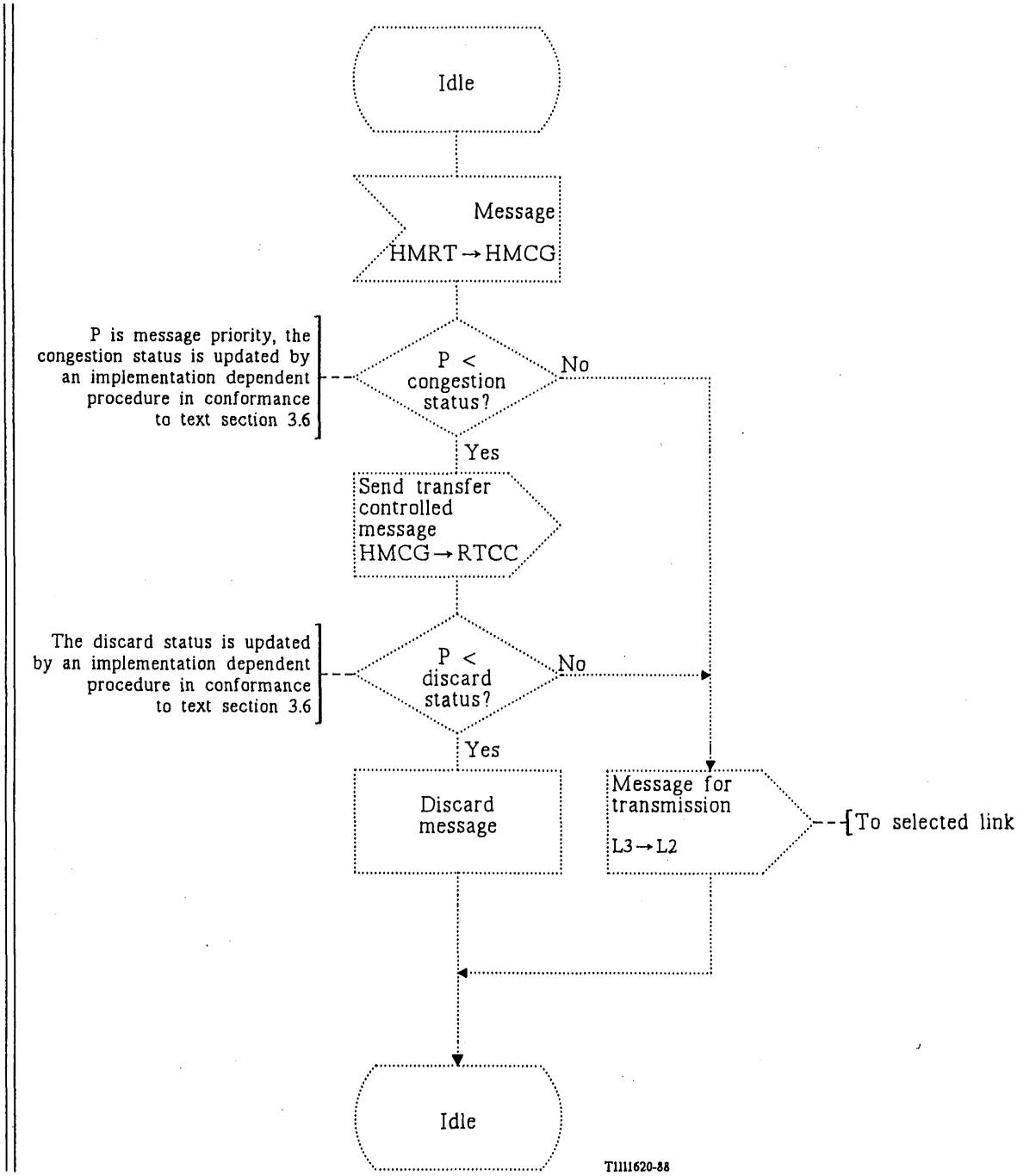
**Signalling message handling ; message routing (HMRT)**




*Note* – Some special routing for MTP Testing User Part may be needed depending on the functions and requirements of such a User Part.

FIGURE 26/Q.704 (Sheet 2 of 2)

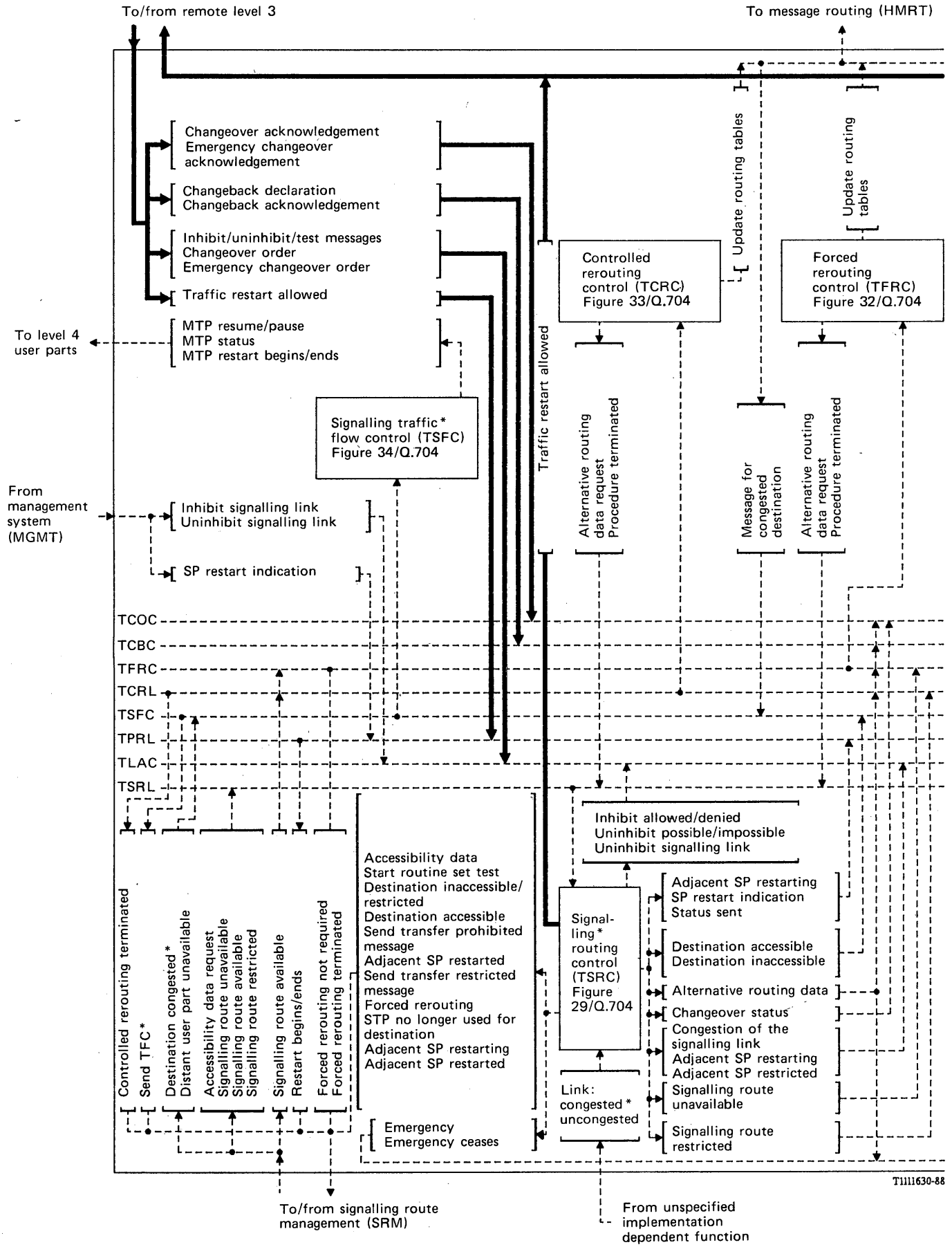
Signalling message handling; message routing (HMRT)




*Note* – Dotted symbols apply only to the multiple congestion states option.

FIGURE 26a/Q.704

**Signalling message handling; signalling link congestion (HMCG)**

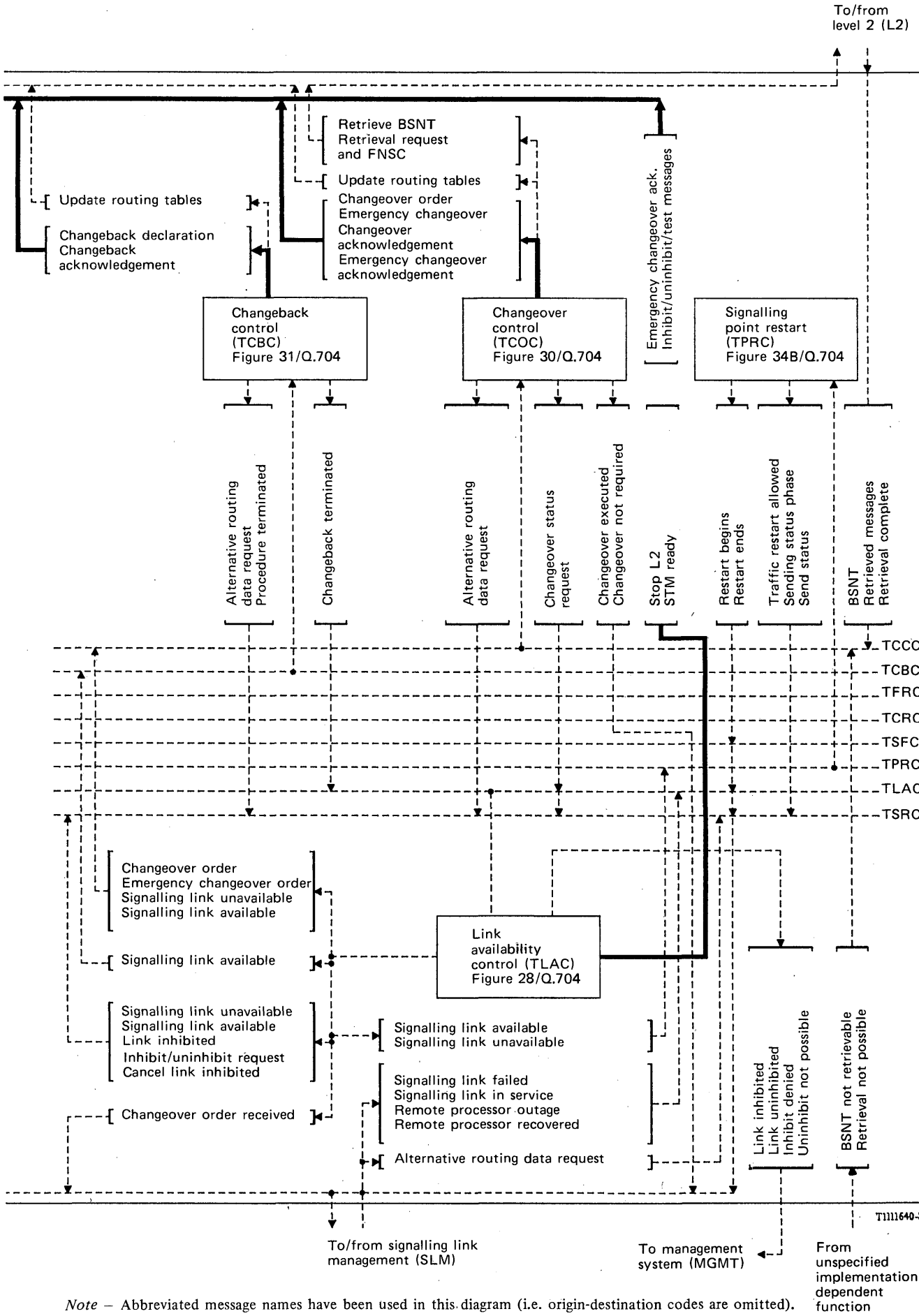



* Functions modified by sheet 3 in case of multiple congestion states.

*Note* – Abbreviated message names have been used in this diagram (i.e. origin-destination codes are omitted).

FIGURE 27/Q.704 (sheet 1 of 3)

**Level 3 – Signalling traffic management (STM); functional block interactions**




*Note* – Abbreviated message names have been used in this diagram (i.e. origin-destination codes are omitted).

FIGURE 27/Q.704 (sheet 2 of 3)

**Level 3 – Signalling traffic management (STM); functional block interactions**

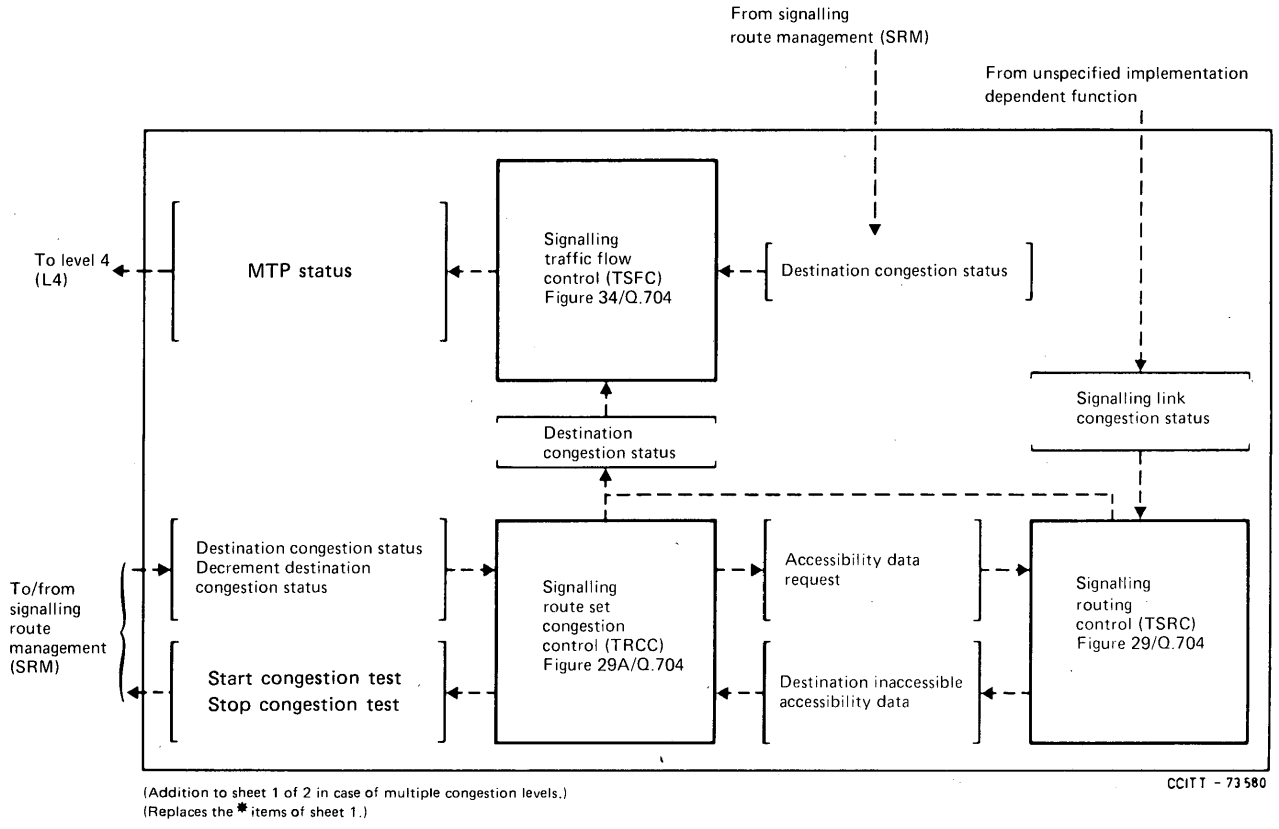



FIGURE 27/Q.704 (sheet 3 of 3)

**Level 3 – Signalling traffic management (STM); functional block interactions**

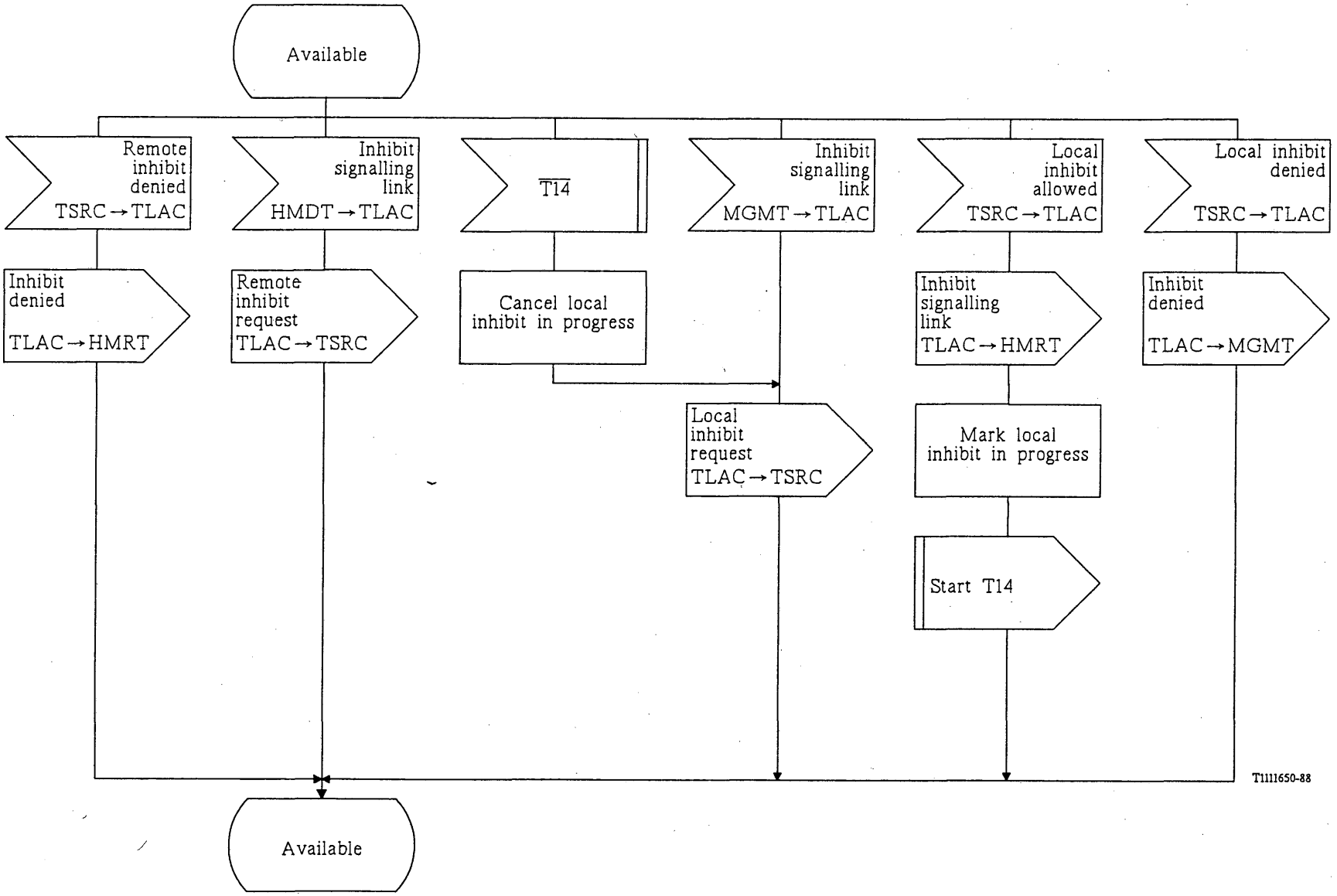



FIGURE 28/Q.704 (Sheet 1 of 17)

**Signalling traffic management; link availability control (TLAC)**

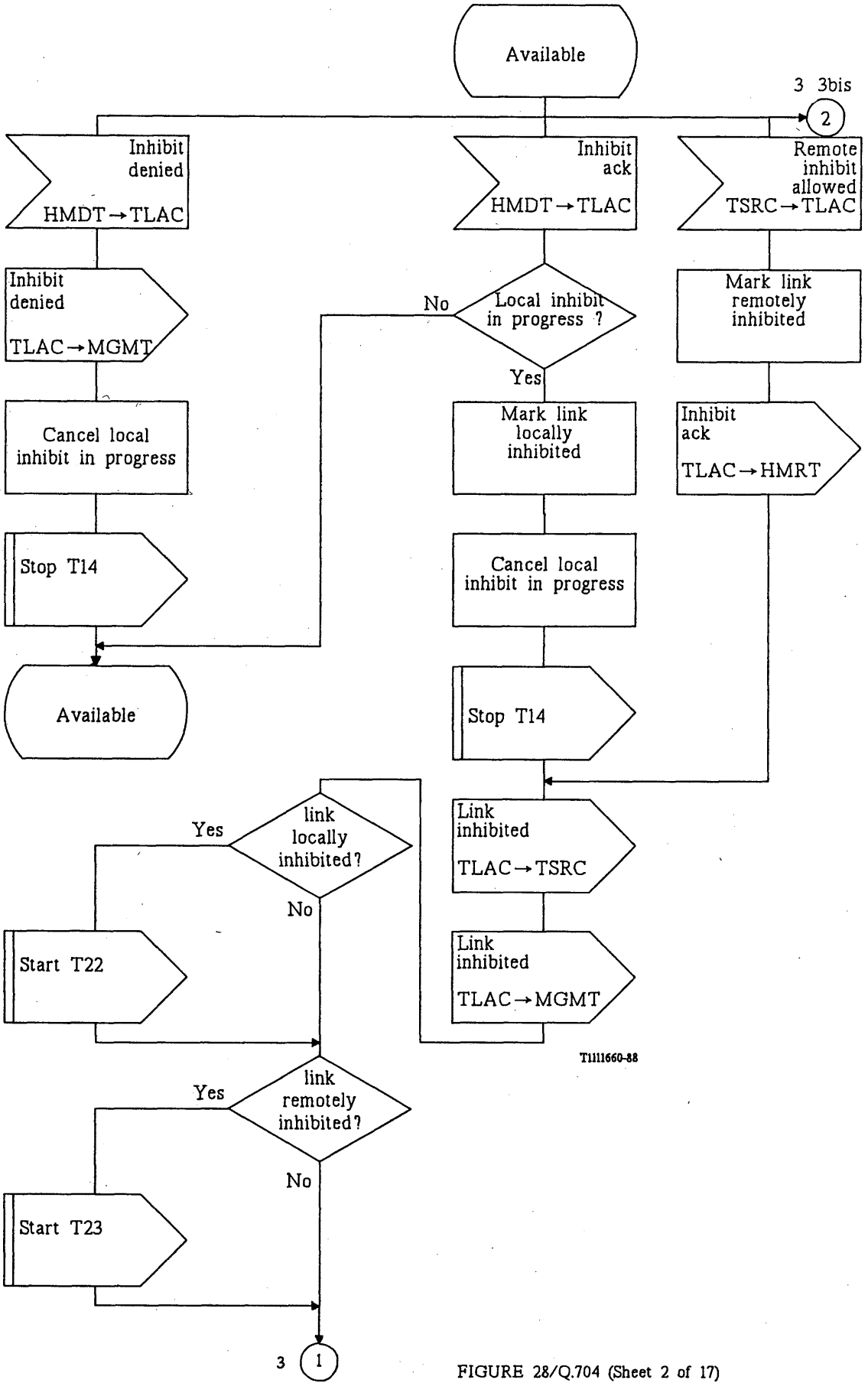



FIGURE 28/Q.704 (Sheet 2 of 17)

**Signalling traffic management; link availability control (TLAC)**

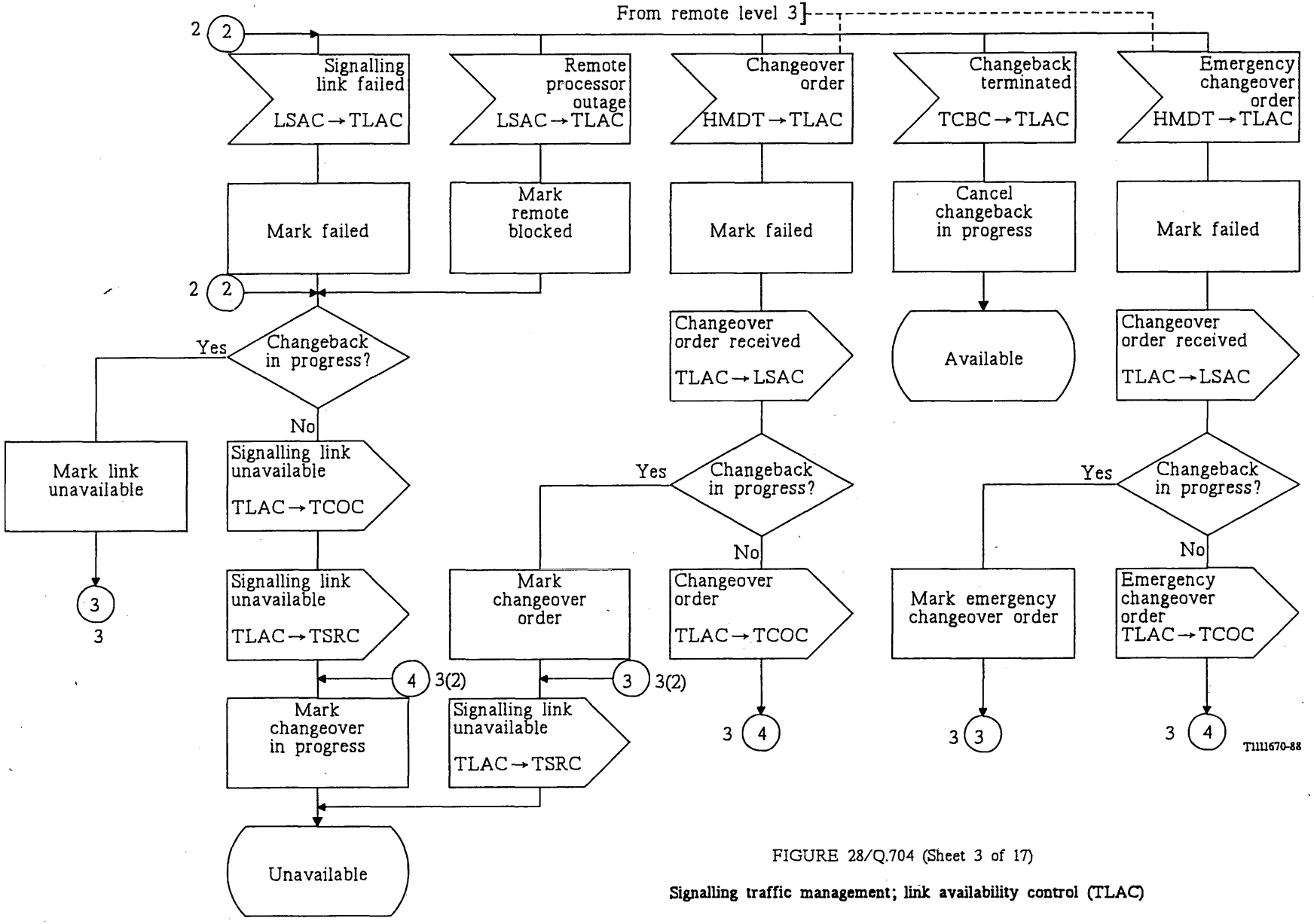



FIGURE 28/Q.704 (Sheet 3 of 17)

**Signalling traffic management; link availability control (TLAC)**

*Note* – See sheet 3bis for national option.

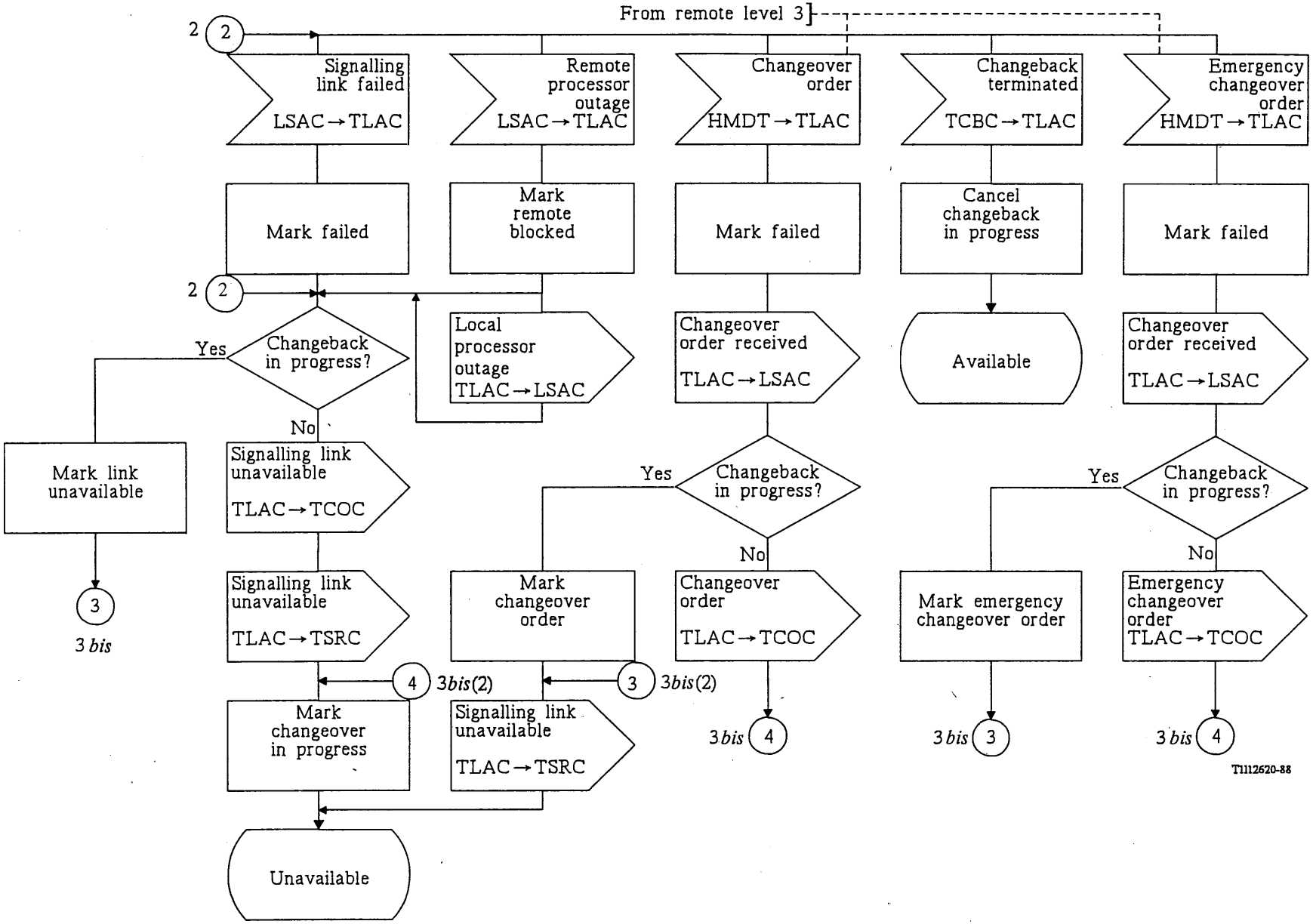
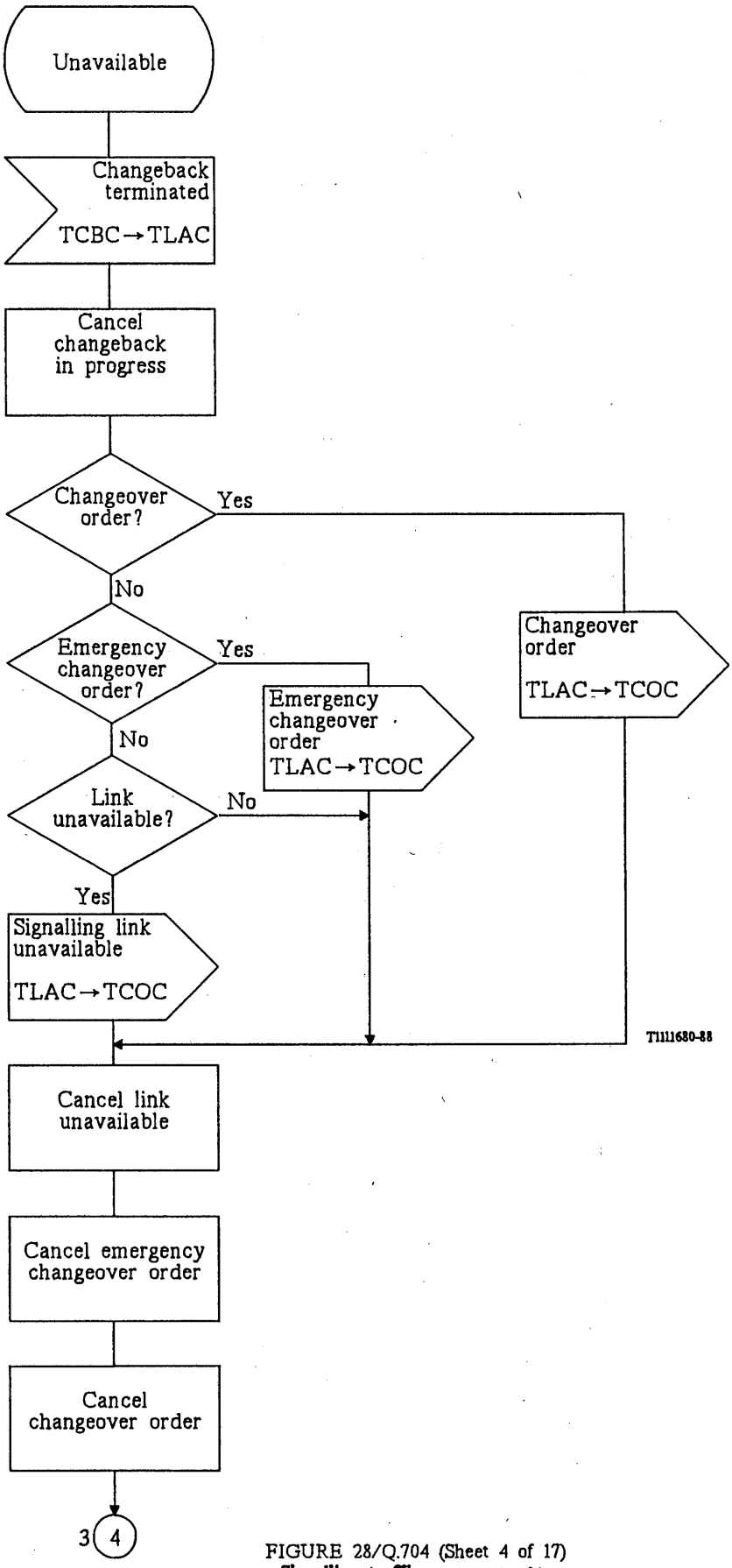



FIGURE 28/Q.704 (sheet 3 *bis* of 17)

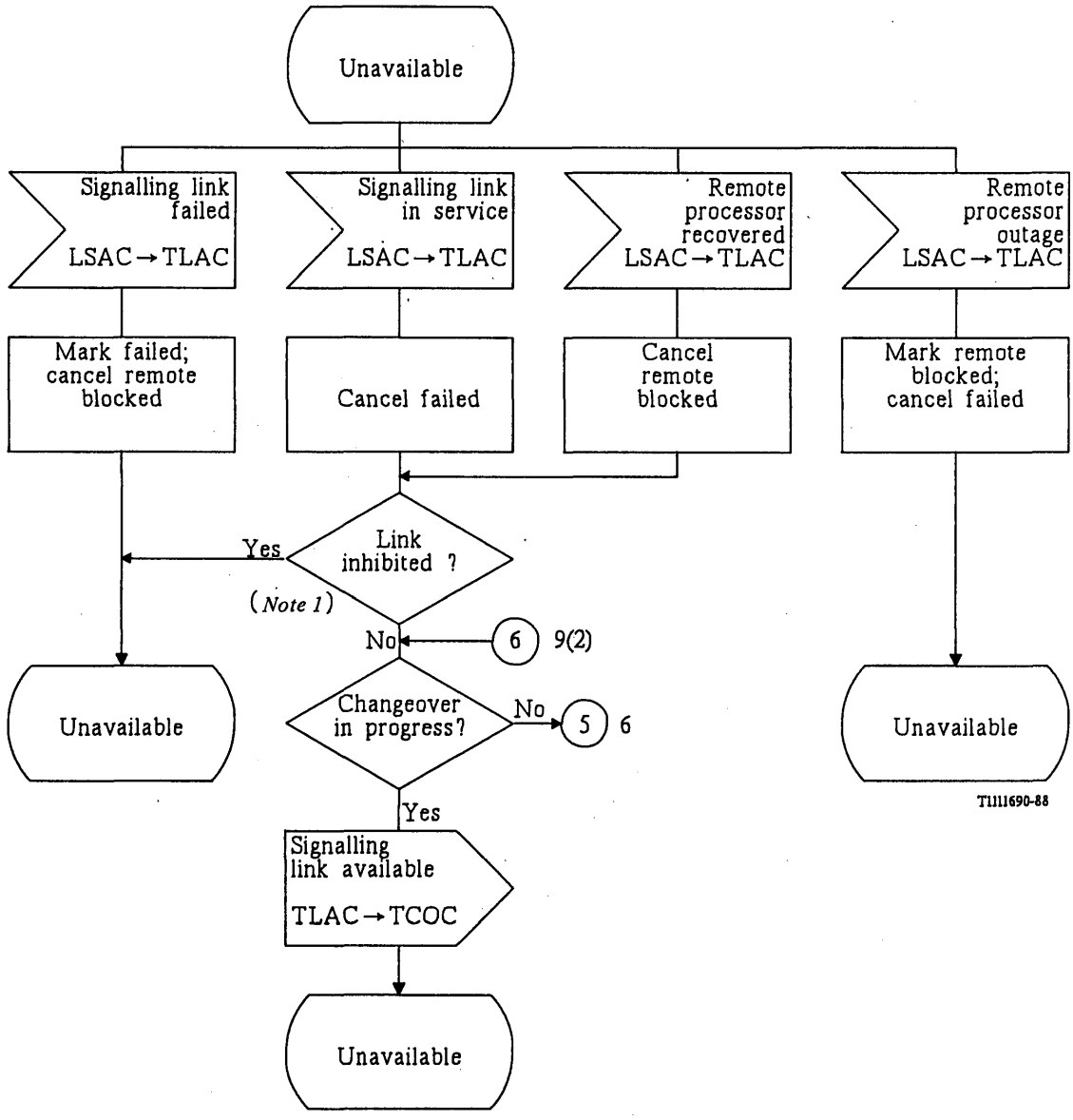
**Signalling traffic management; link availability control (TLAC)**

(National option)




4

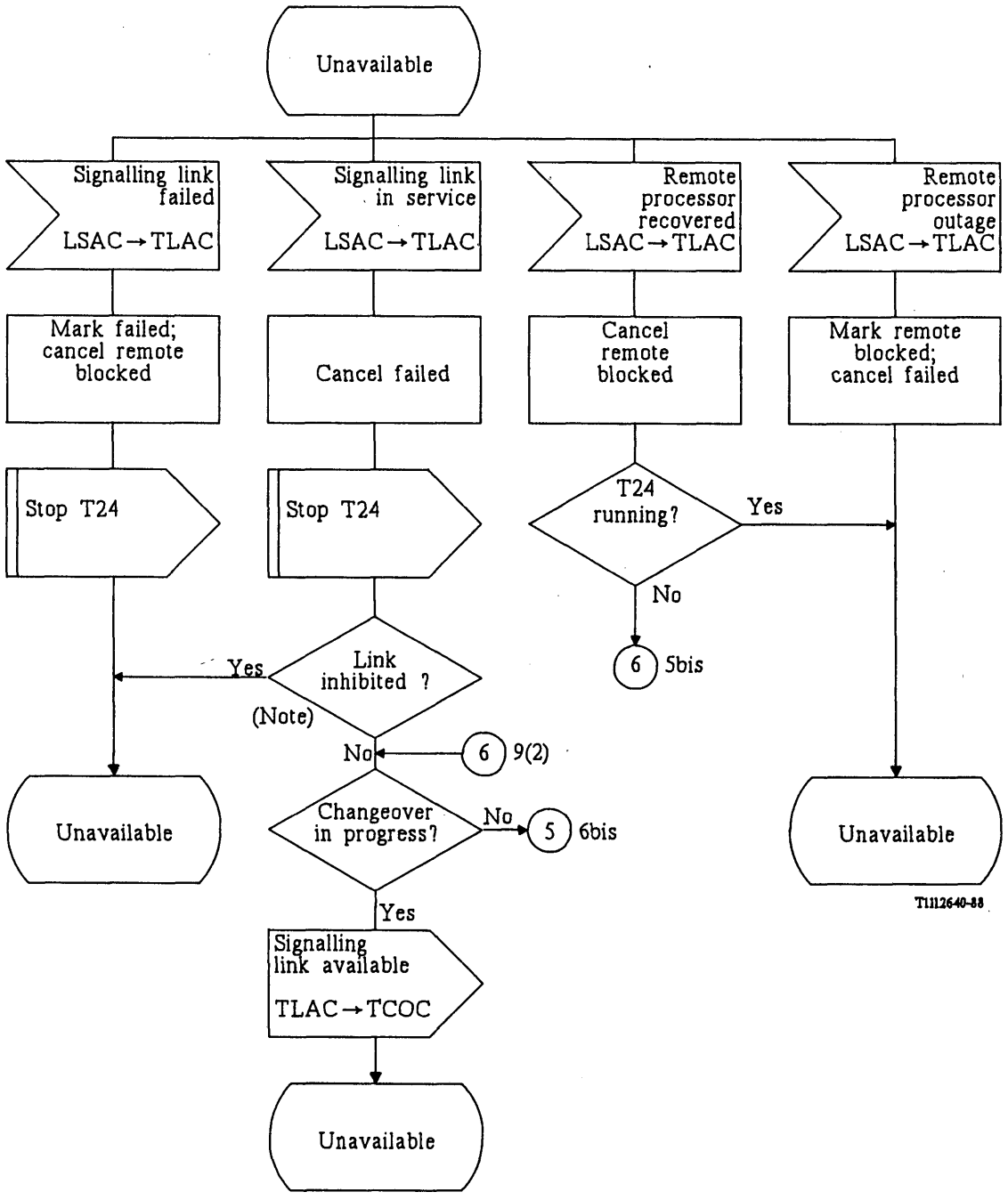
FIGURE 28/Q.704 (Sheet 4 of 17)
**Signalling traffic management; link availability control (TLAC)**




*Note 1* – "Inhibited" indicates either locally or remotely inhibited, or both.
*Note 2* – See sheet *5bis*, for national option.

FIGURE 28/Q.704 (Sheet 5 of 17)

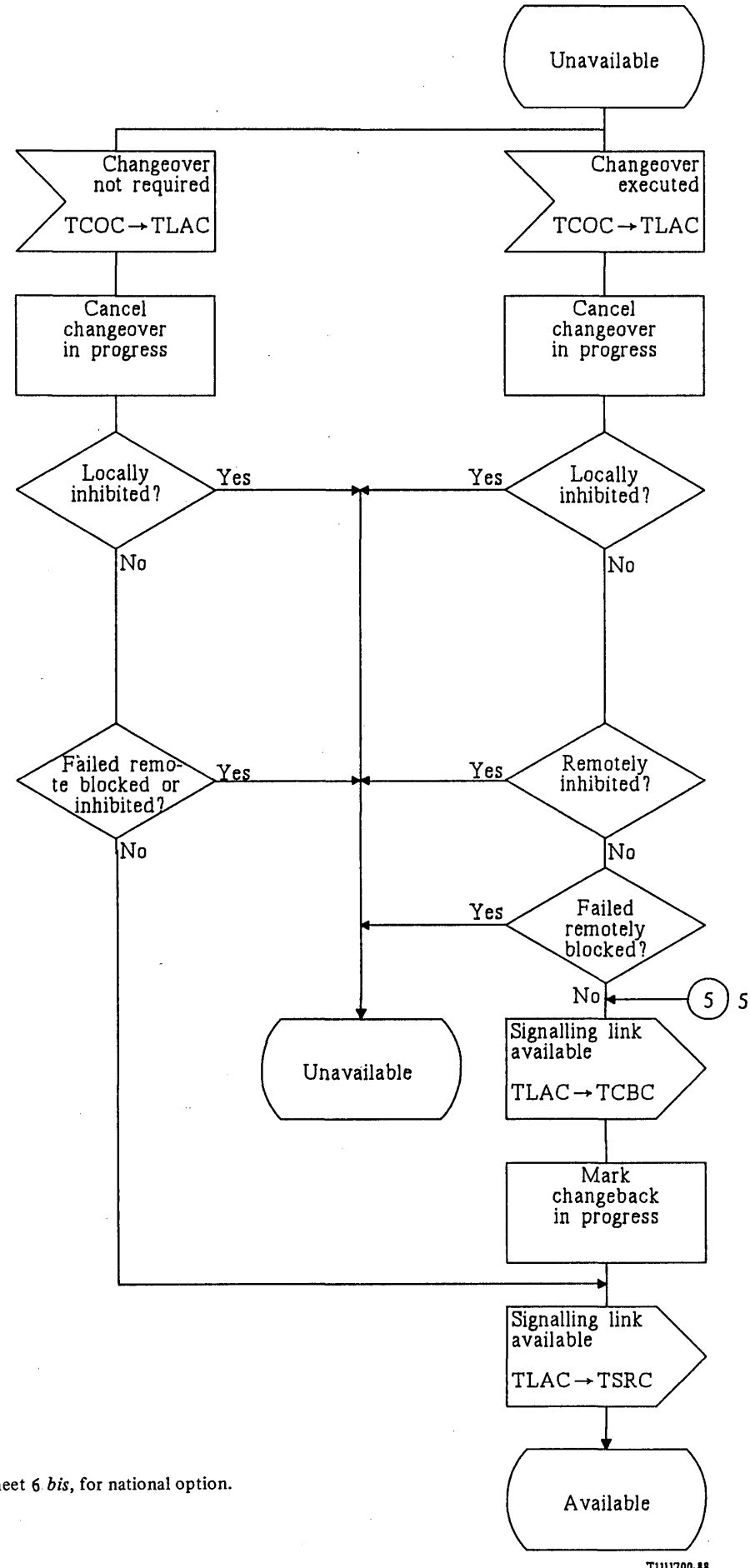
**Signalling traffic management; link availability control (TLAC)**




*Note* – "Inhibited" indicates either locally or remotely inhibited, or both.

FIGURE 28/Q.704 (sheet 5 *bis* of 17)

**Signalling traffic management; link availability control (TLAC)**
(National option)




5

See sheet 6 *bis*, for national option.

FIGURE 28/Q.704 (Sheet 6 of 17)
**Signalling traffic management; link availability control (TLAC)**

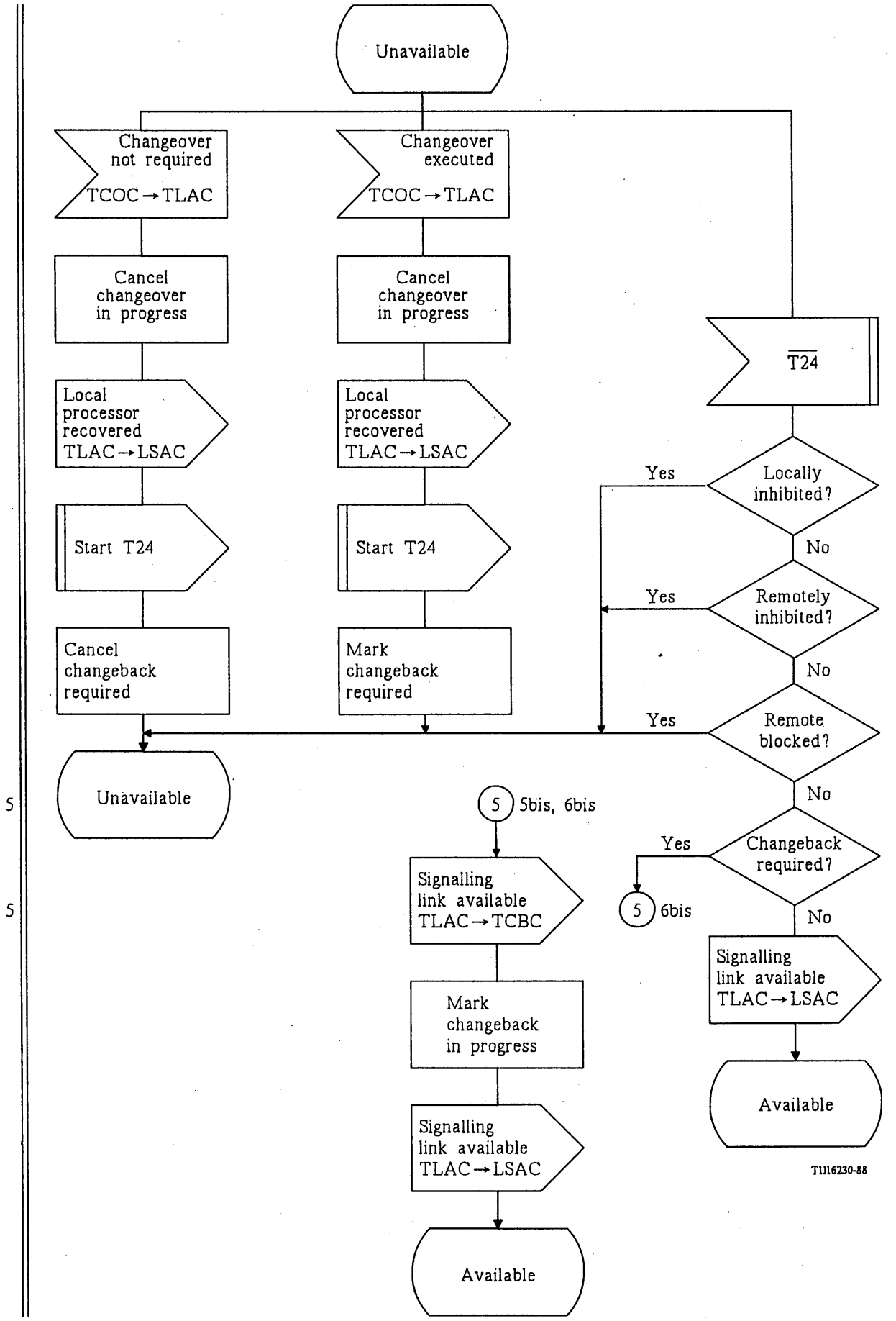



FIGURE 28/Q.704 (sheet 6 *bis* of 17)

**Signalling traffic management; link availability control (TLAC)**

(National option)

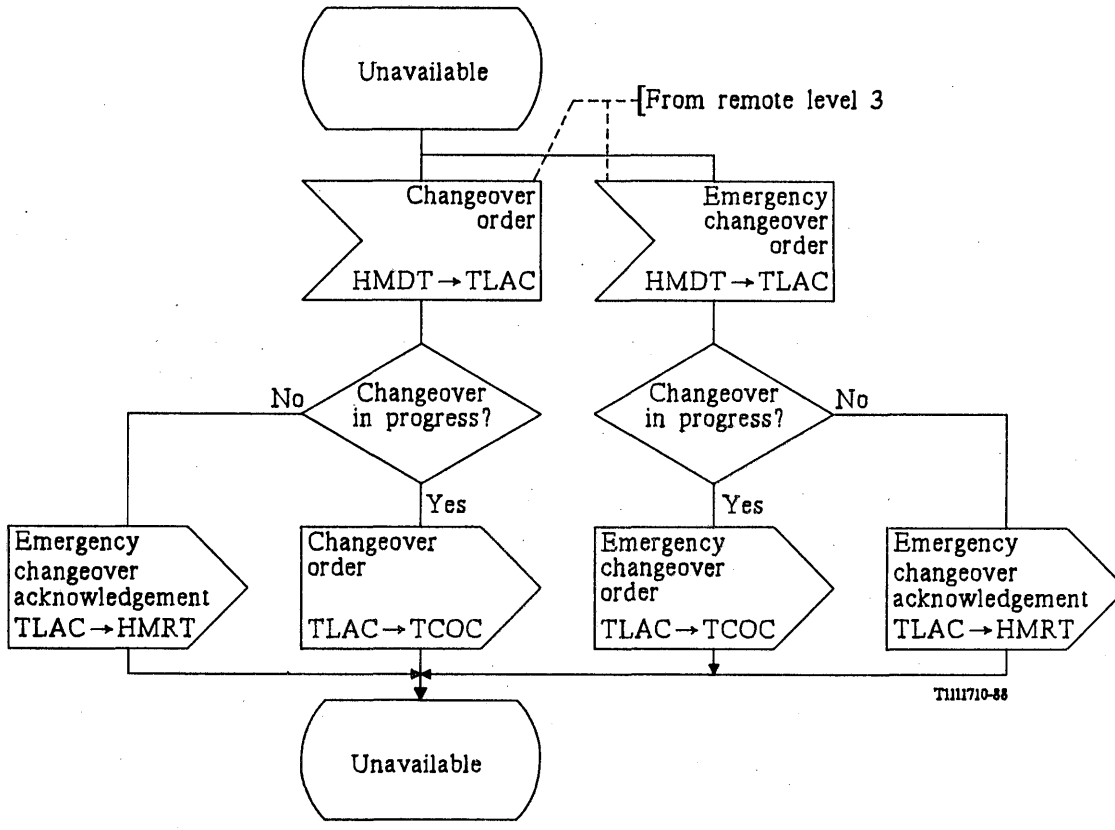
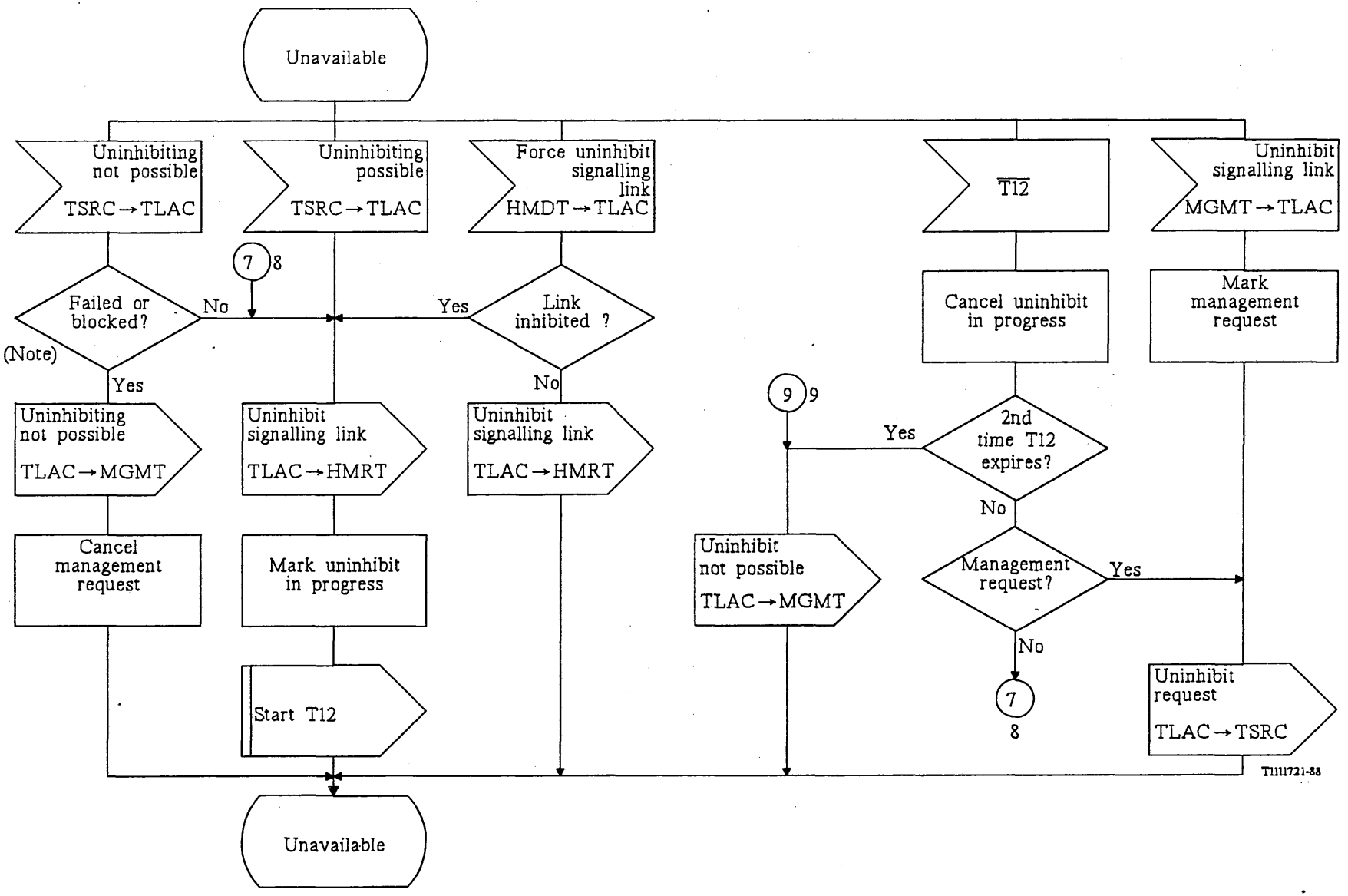



FIGURE 28/Q.704 (Sheet 7 of 17)

**Signalling traffic management; link availability control (TLAC)**




*Note* – "Blocked" indicates remote blocked.

FIGURE 28/Q.704 (Sheet 8 of 17)

**Signalling traffic management; link availability control (TLAC)**

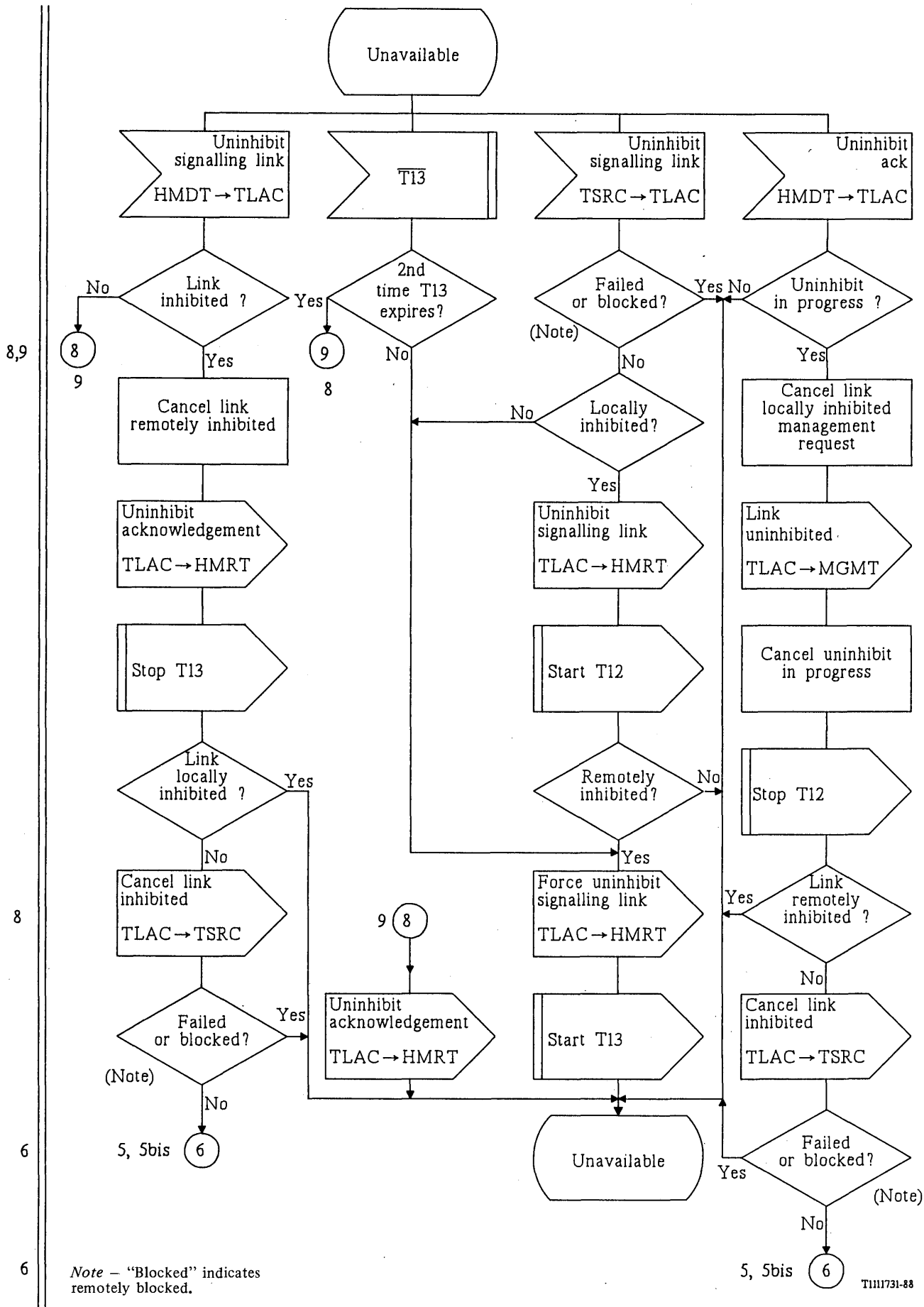



FIGURE 28/Q.704 (Sheet 9 of 17)

**Signalling traffic management; link availability control (TLAC)**

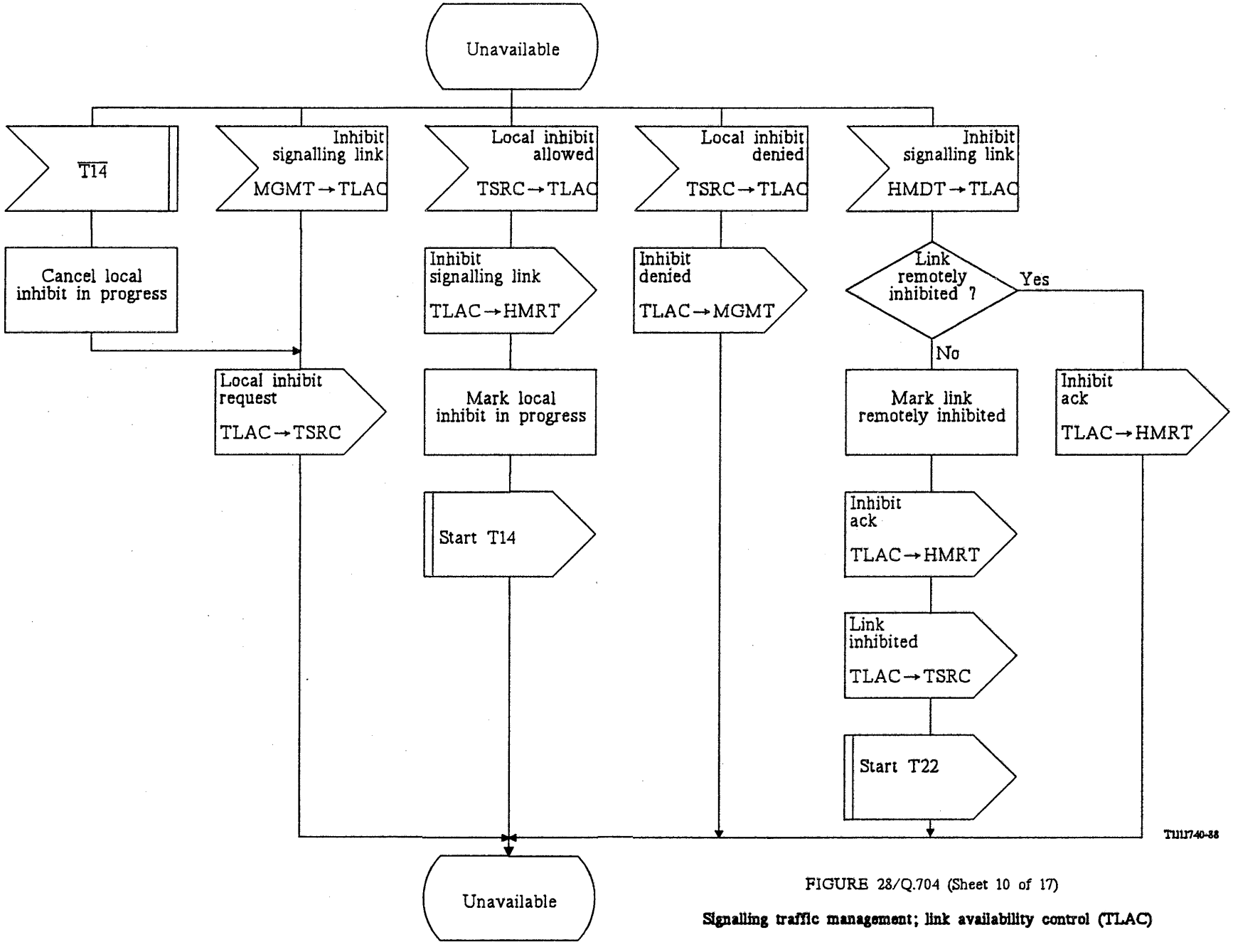



FIGURE 28/Q.704 (Sheet 10 of 17)

**Signalling traffic management; link availability control (TLAC)**

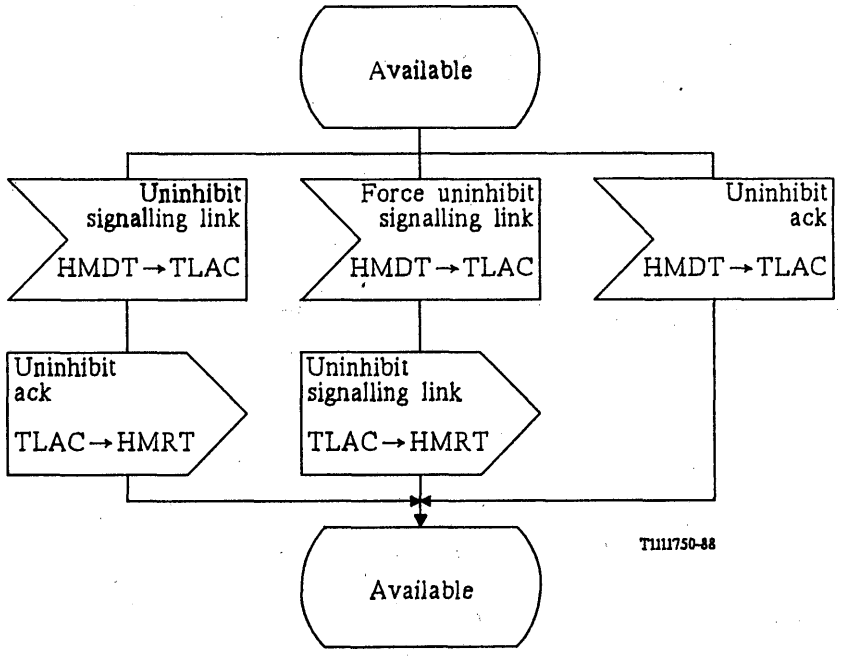



FIGURE 28/Q.704 (Sheet 11 of 17)

**Signalling traffic management; link availability control (TLAC)**

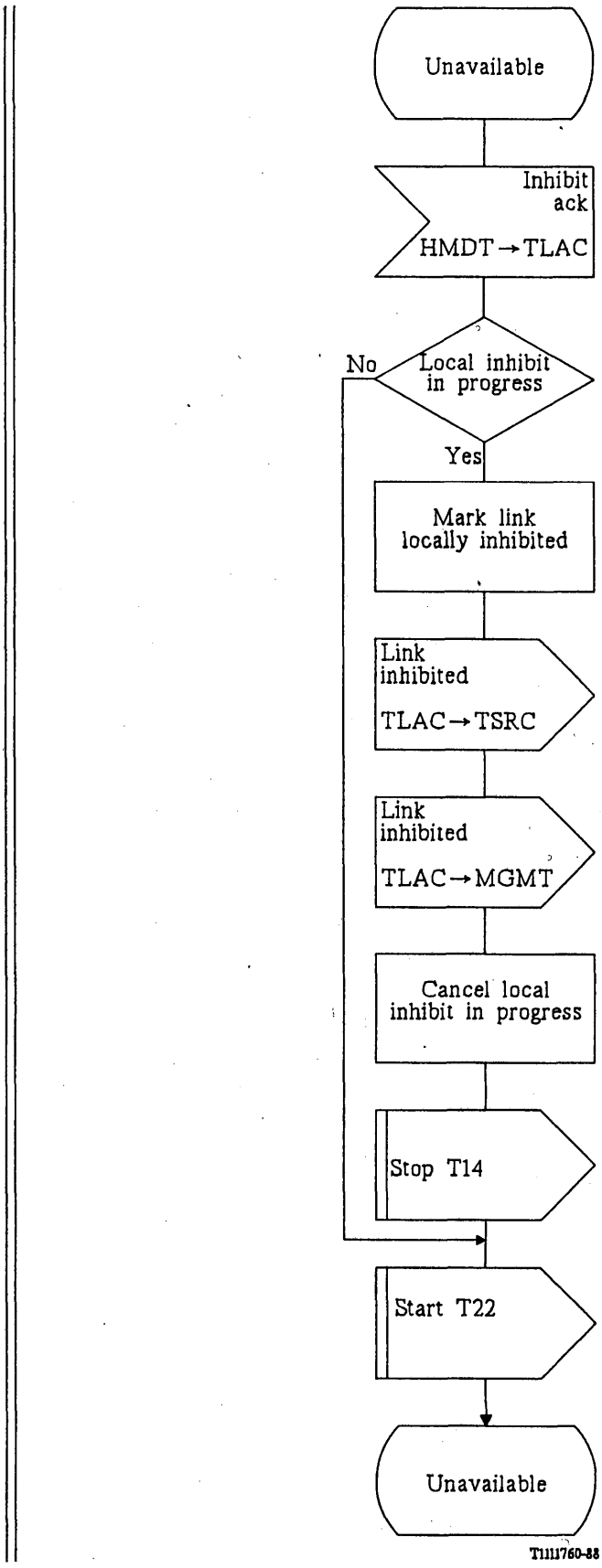



FIGURE 28/Q.704 (Sheet 12 of 17)

**Signalling traffic management; link availability control (TLAC)**

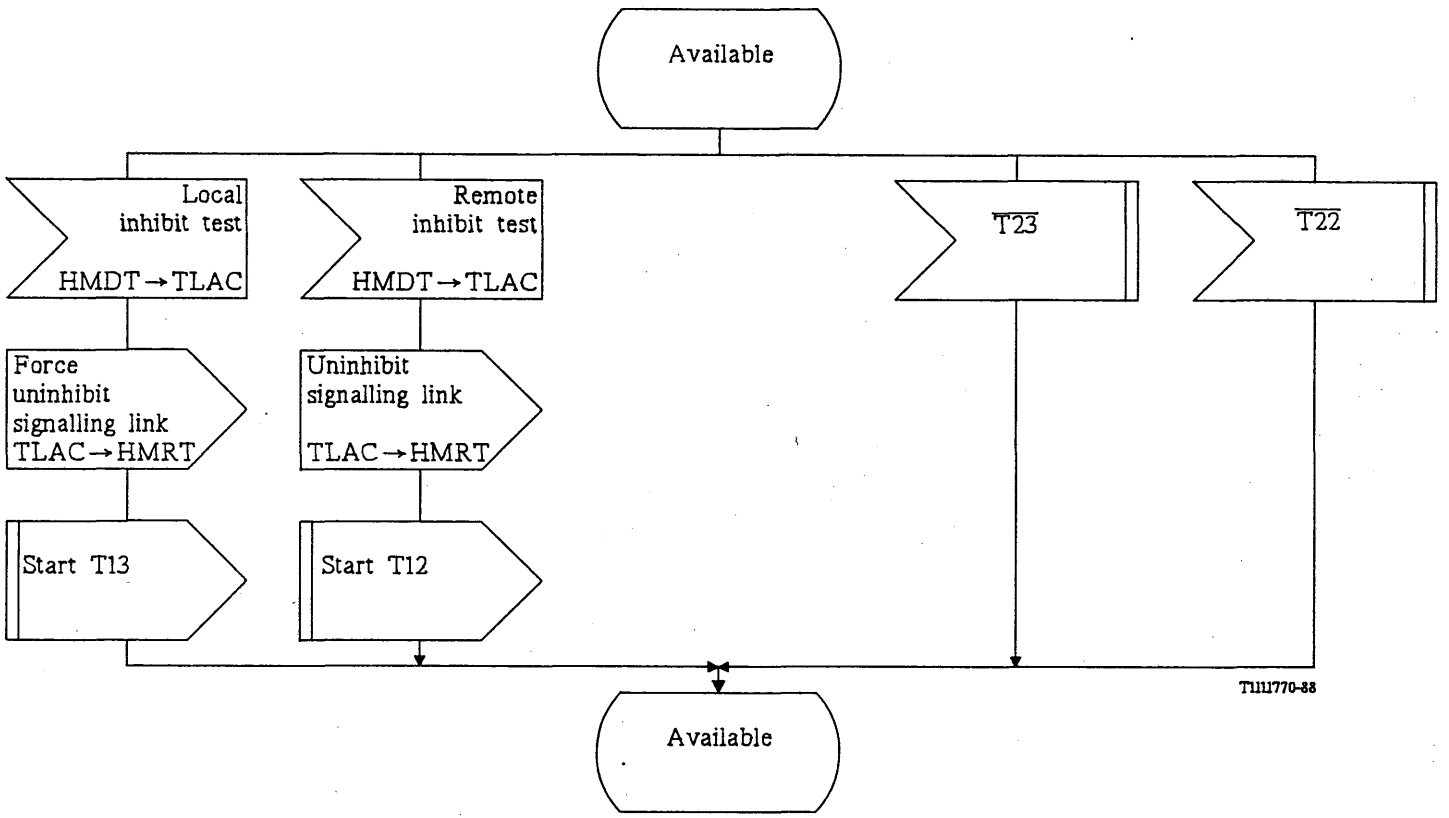



FIGURE 28/Q.704 (Sheet 13 of 17)

**Signalling traffic management; link availability control (TLAC)**

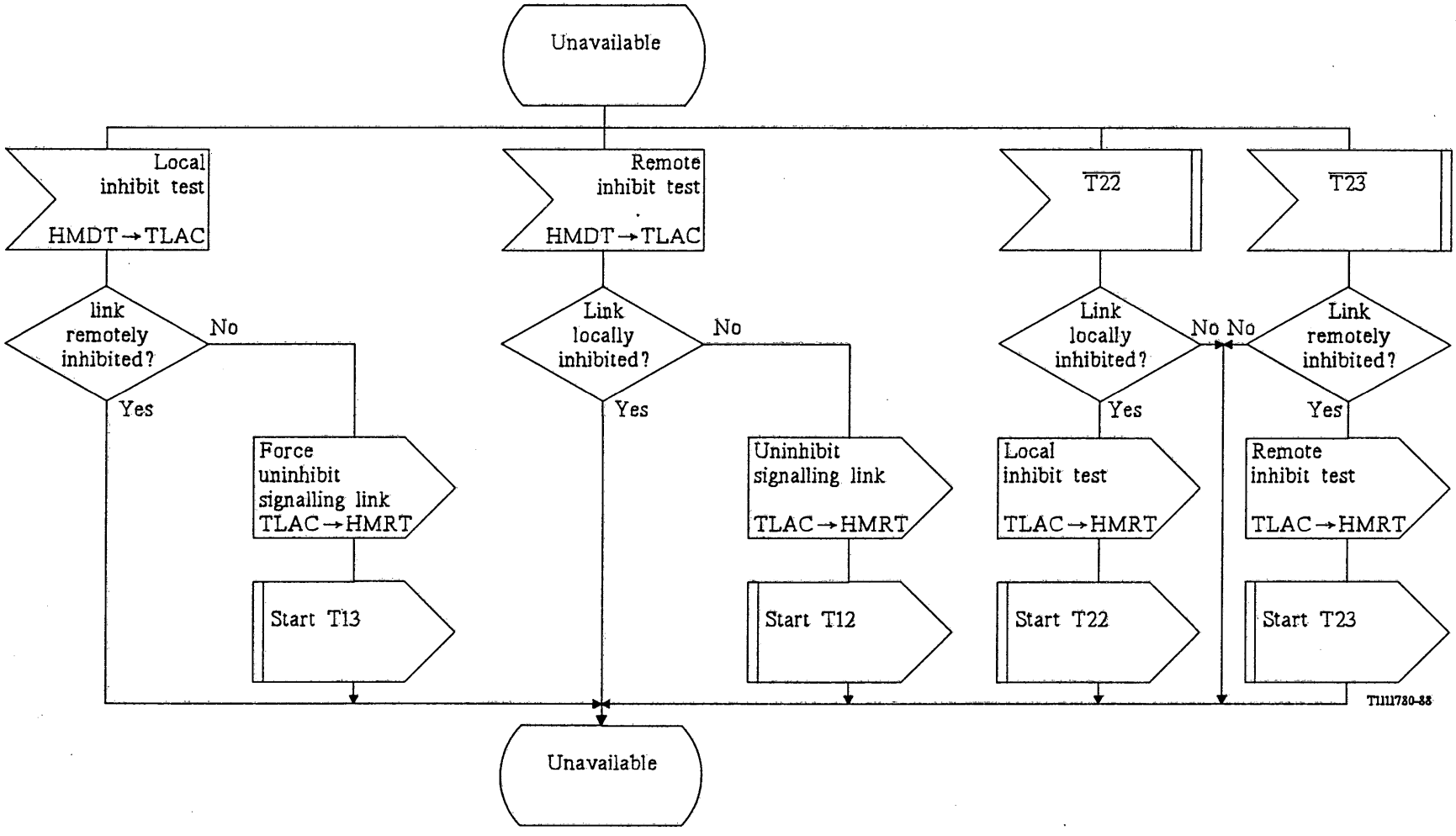



FIGURE 28/Q.704 (sheet 14 of 17)

**Signalling traffic management; link availability control (TLAC)**

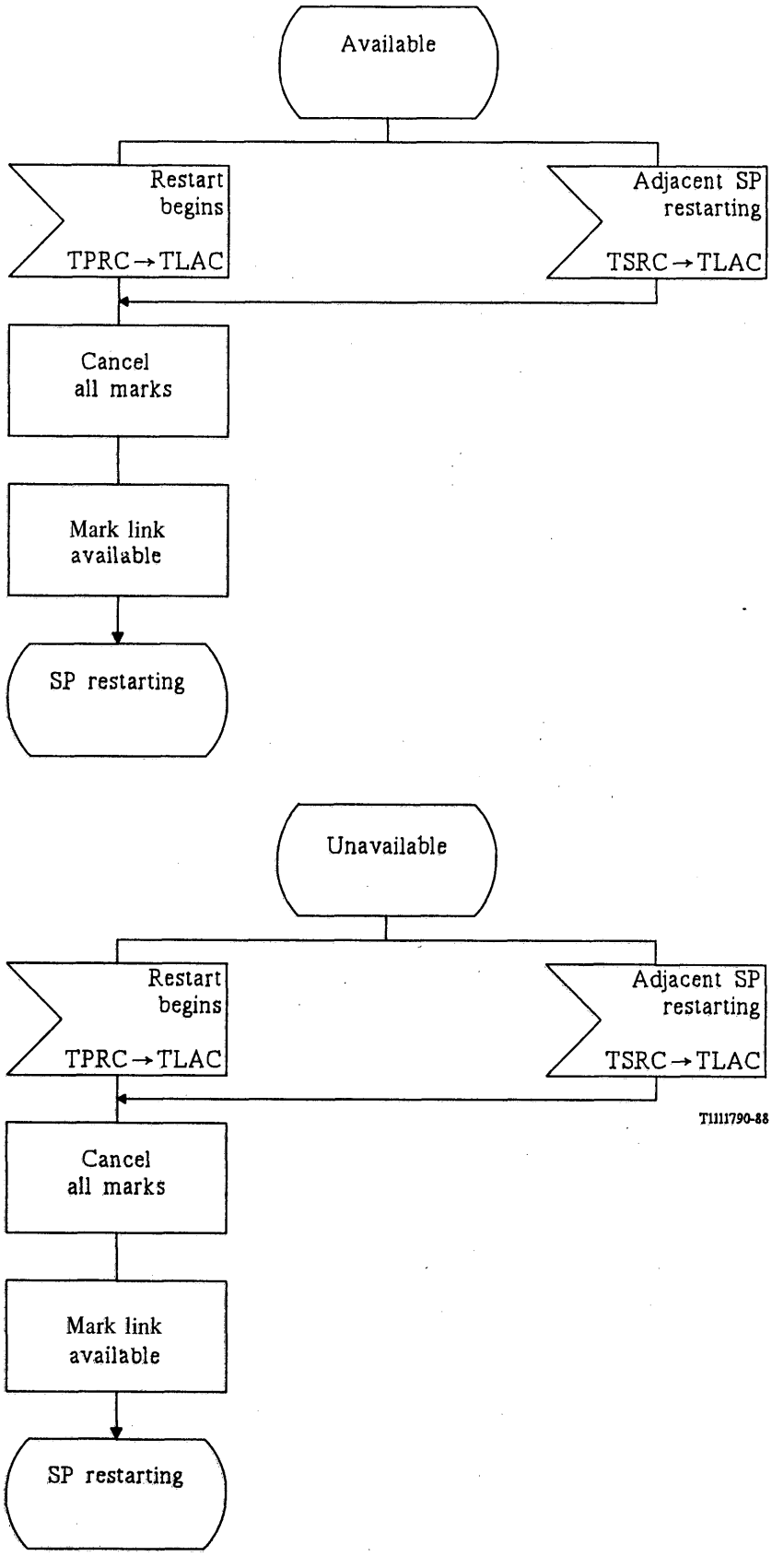



FIGURE 28/Q.704 (Sheet 15 of 17)

**Signalling traffic management; link availability control (TLAC)**

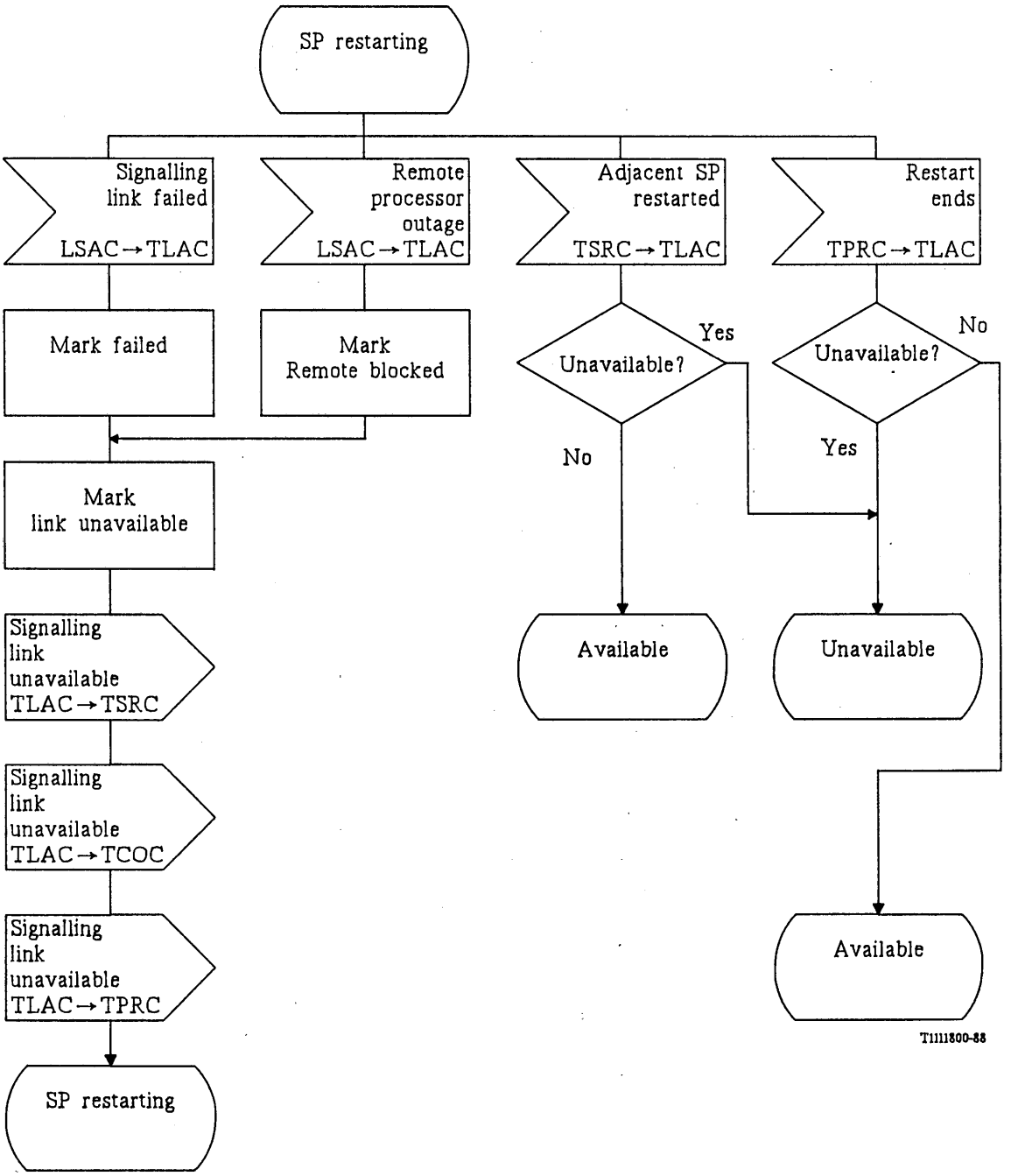



FIGURE 28/Q.704 (Sheet 16 of 17)

**Signalling traffic management; link availability control (TLAC)**

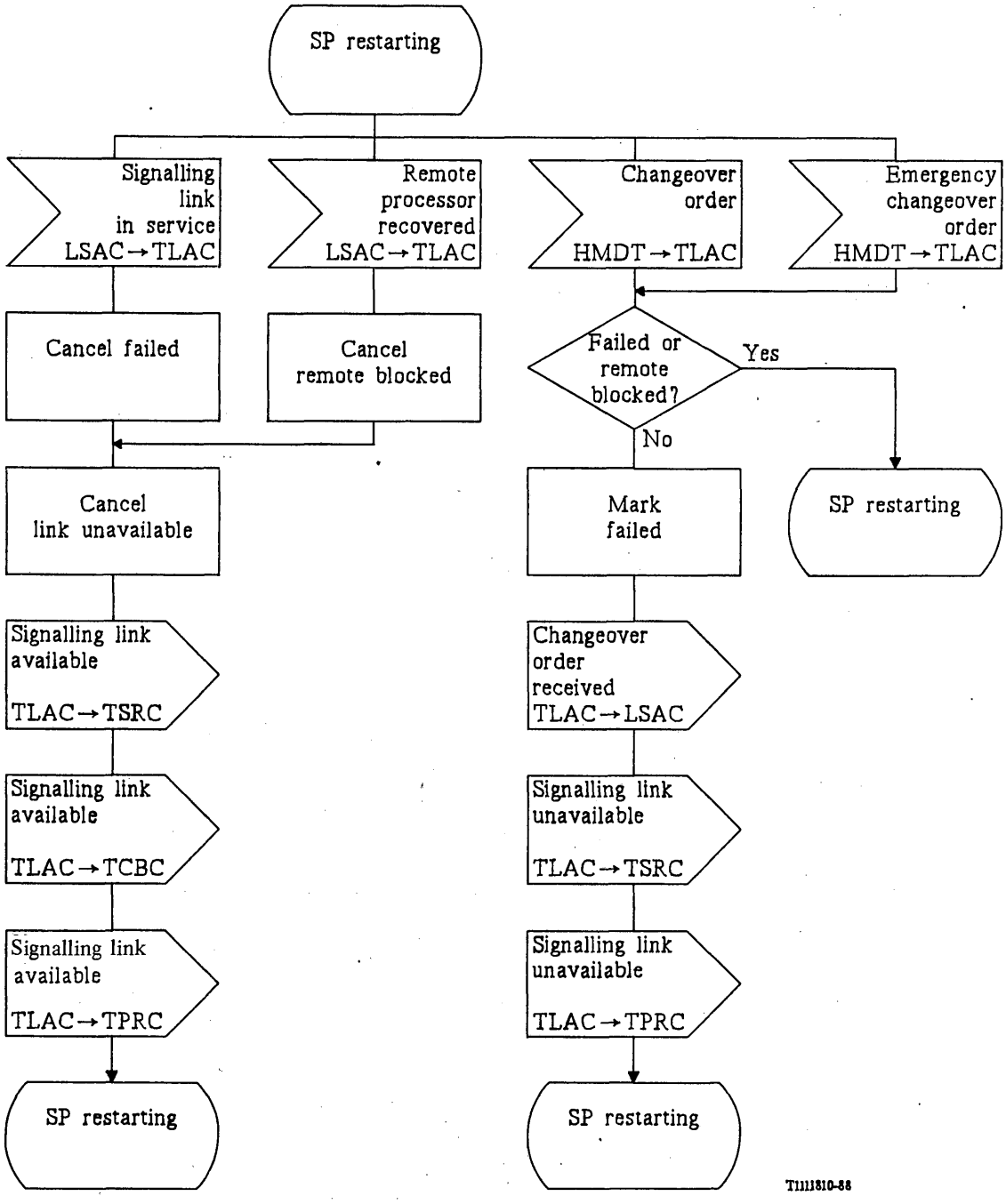



FIGURE 28/Q.704 (Sheet 17 of 17)

**Signalling traffic management; link availability control (TLAC)**

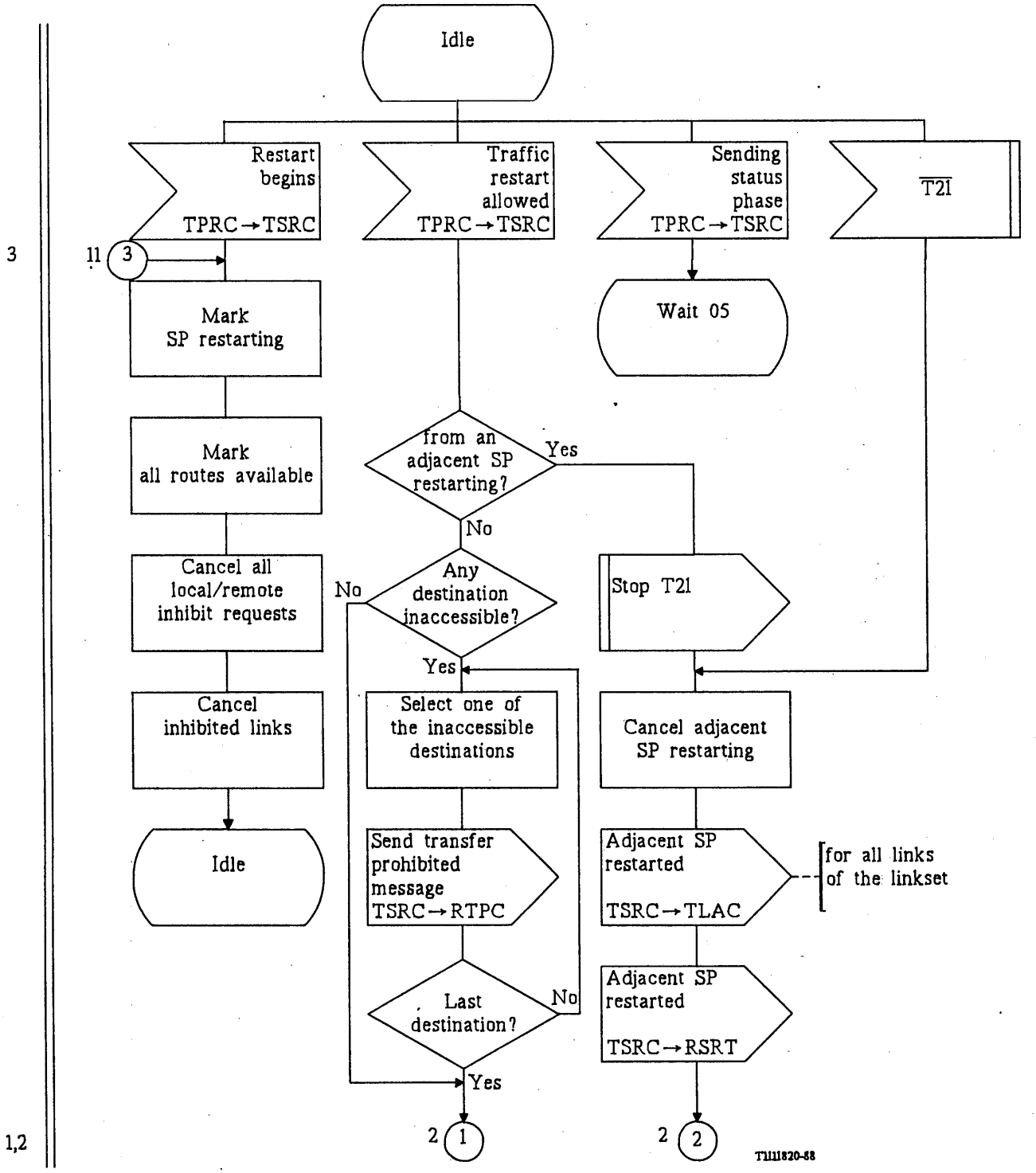



FIGURE 29/Q.704 (Sheet 1 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

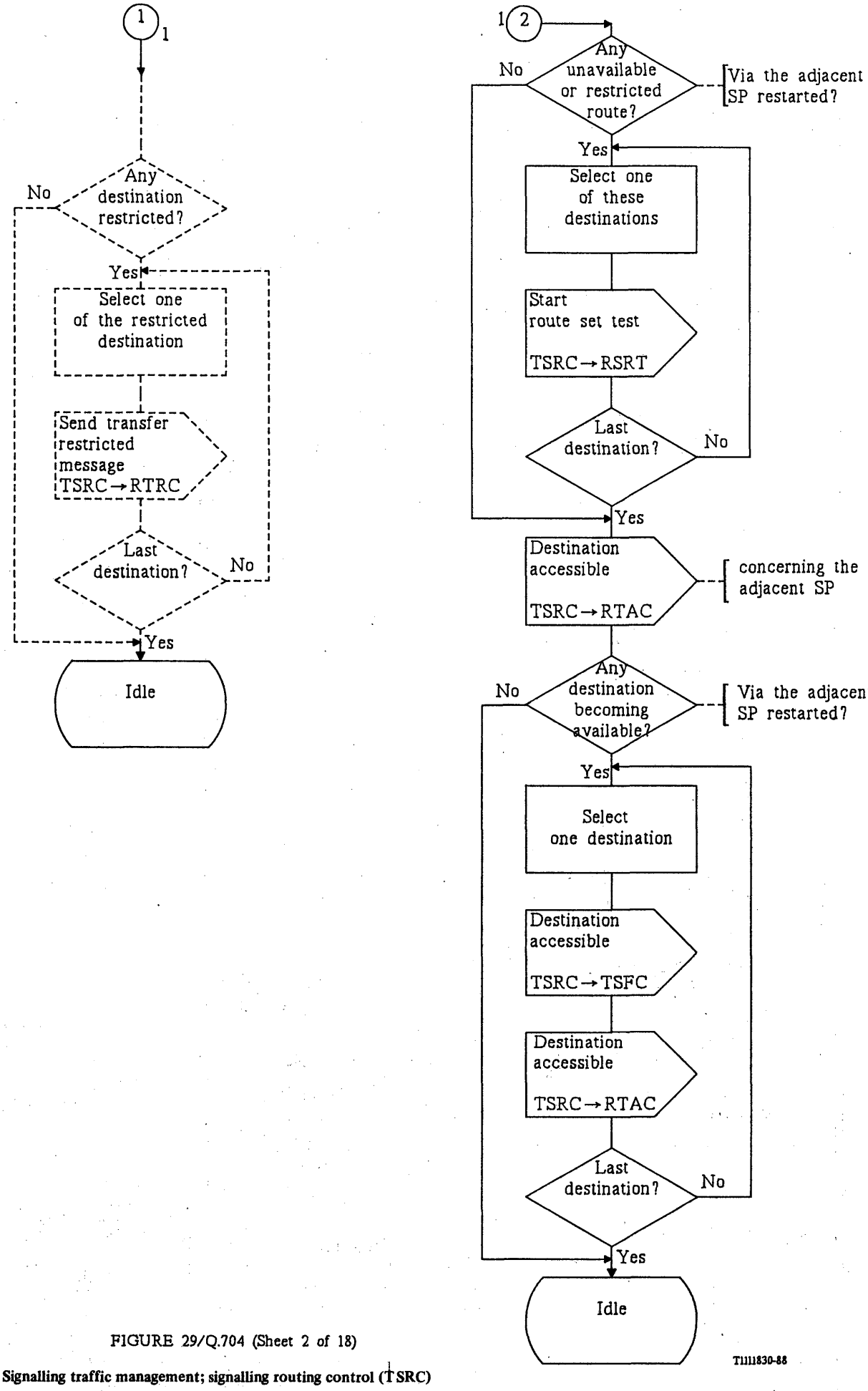



FIGURE 29/Q.704 (Sheet 2 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

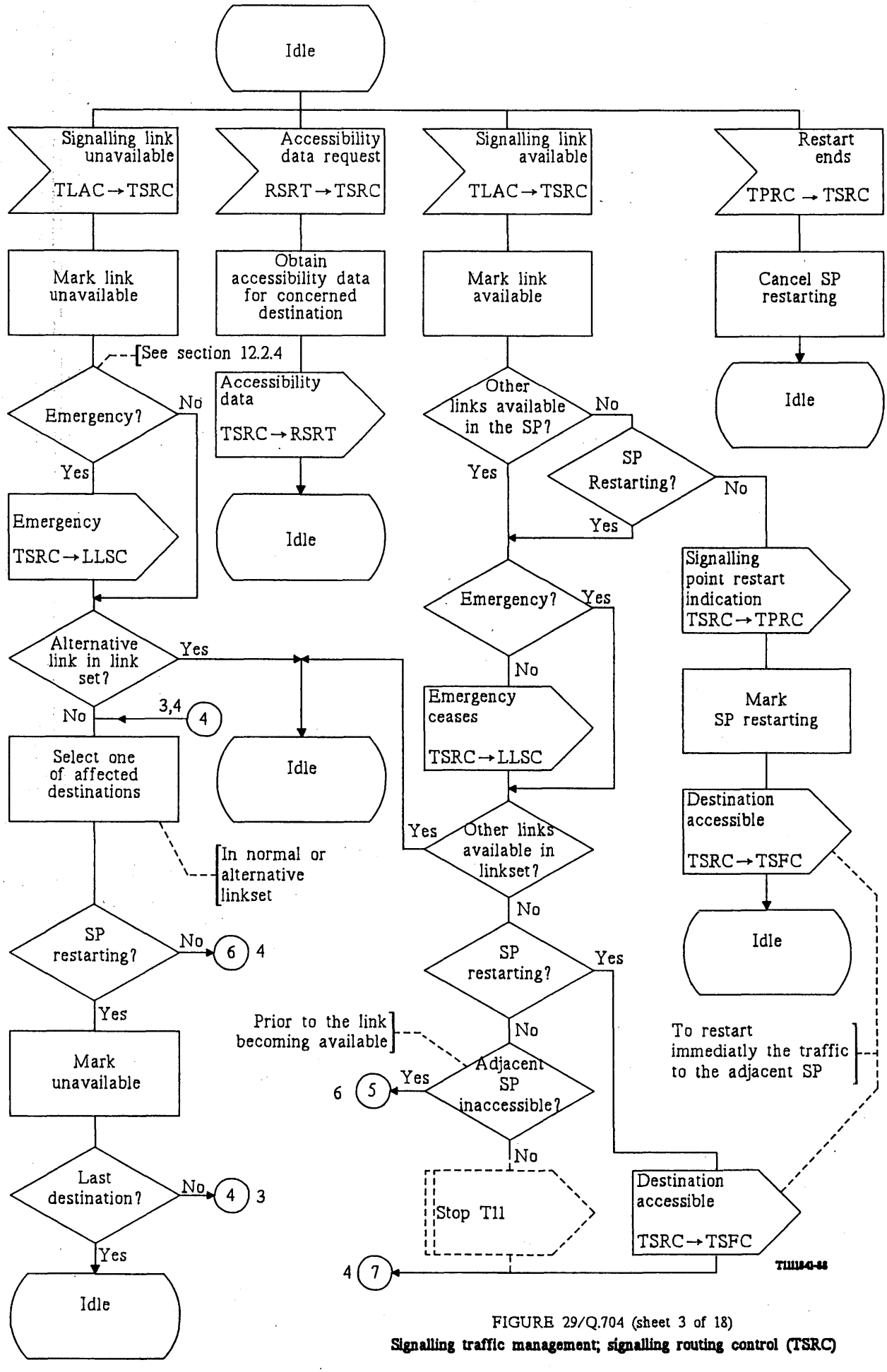
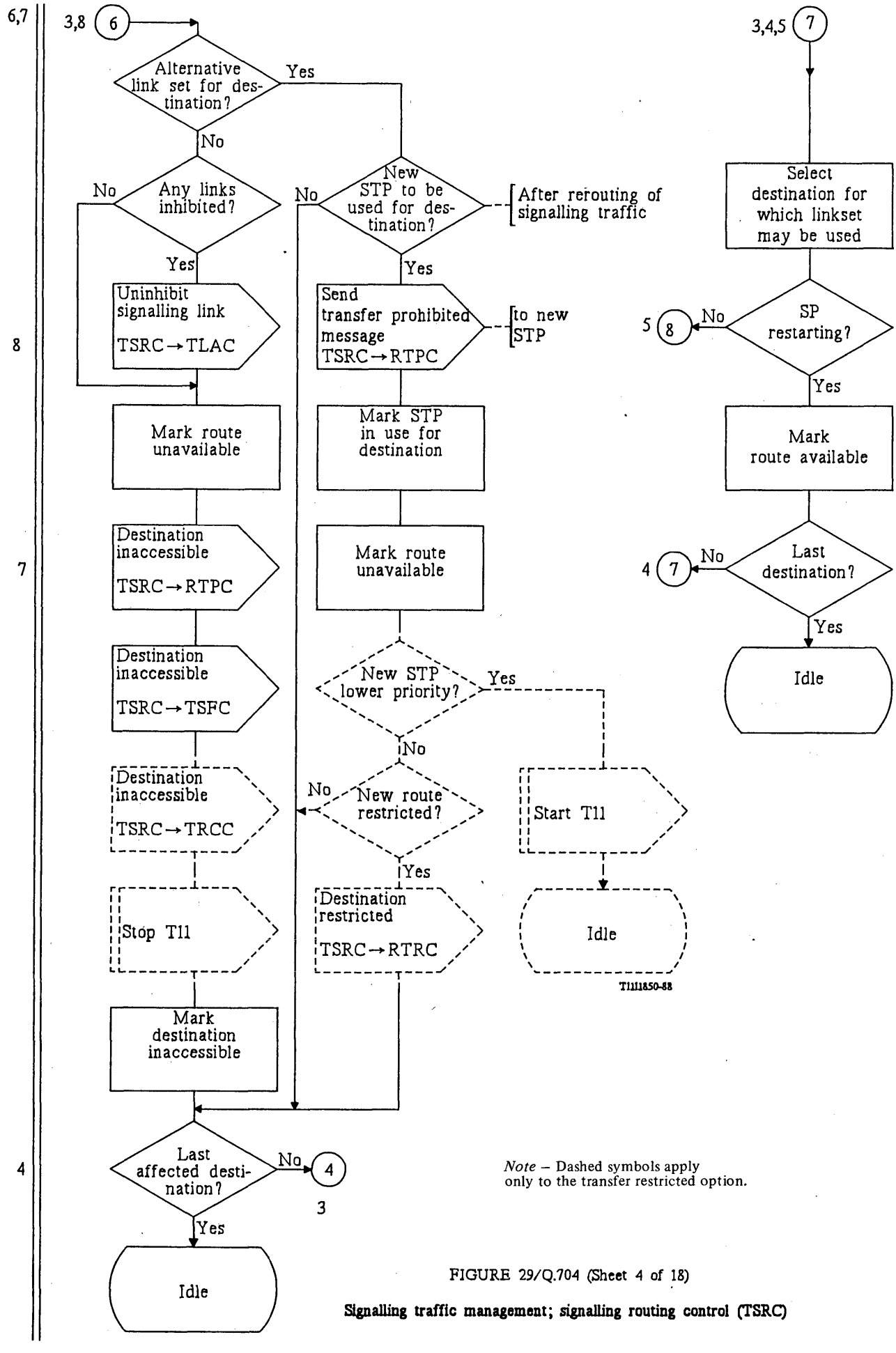



FIGURE 29/Q.704 (sheet 3 of 18)

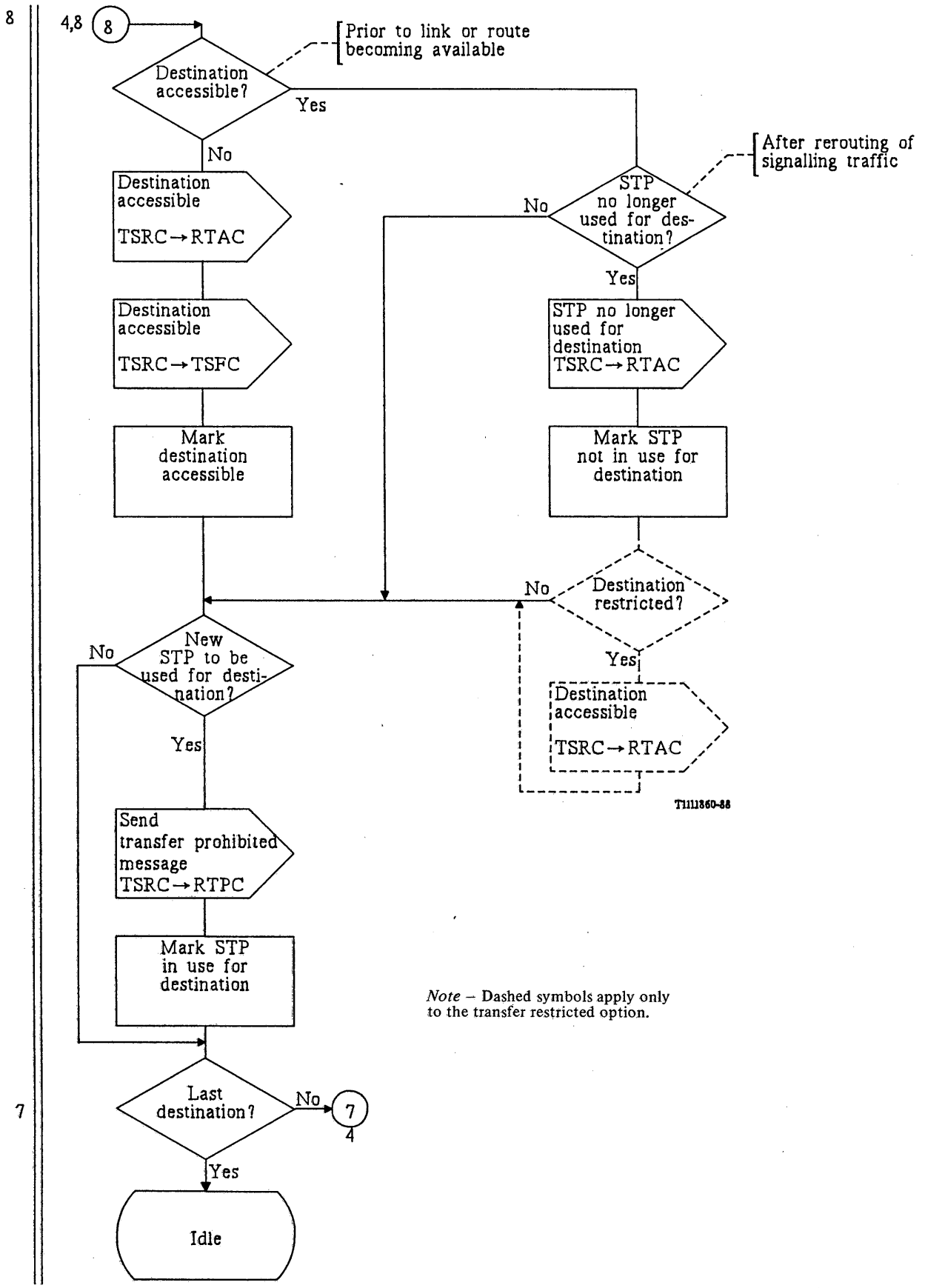
**Signalling traffic management; signalling routing control (TSRC)**




*Note* – Dashed symbols apply only to the transfer restricted option.

FIGURE 29/Q.704 (Sheet 4 of 18)

**Signalling traffic management; signalling routing control (TSRC)**




*Note* – Dashed symbols apply only to the transfer restricted option.

FIGURE 29/Q.704 (Sheet 5 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

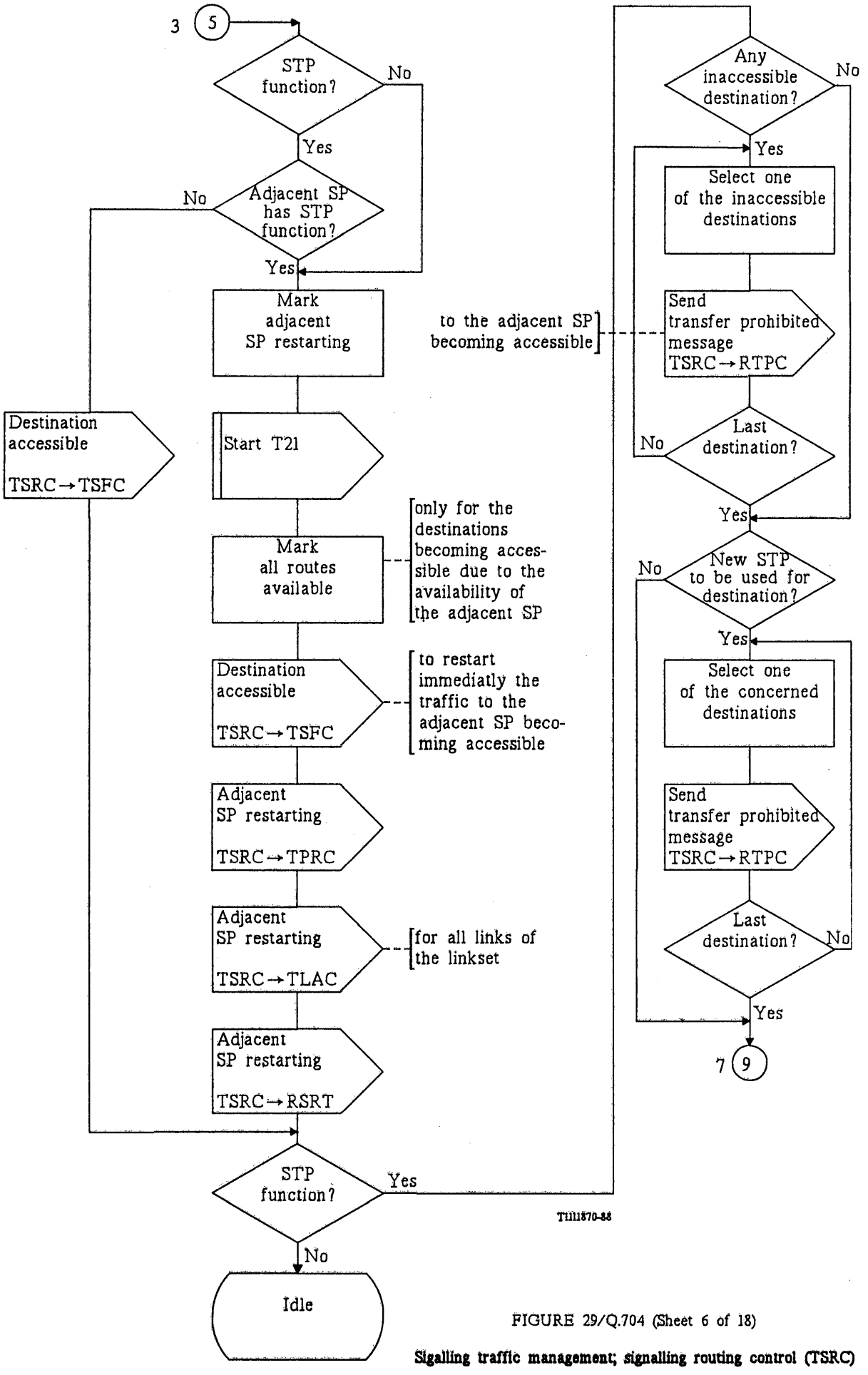



FIGURE 29/Q.704 (Sheet 6 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

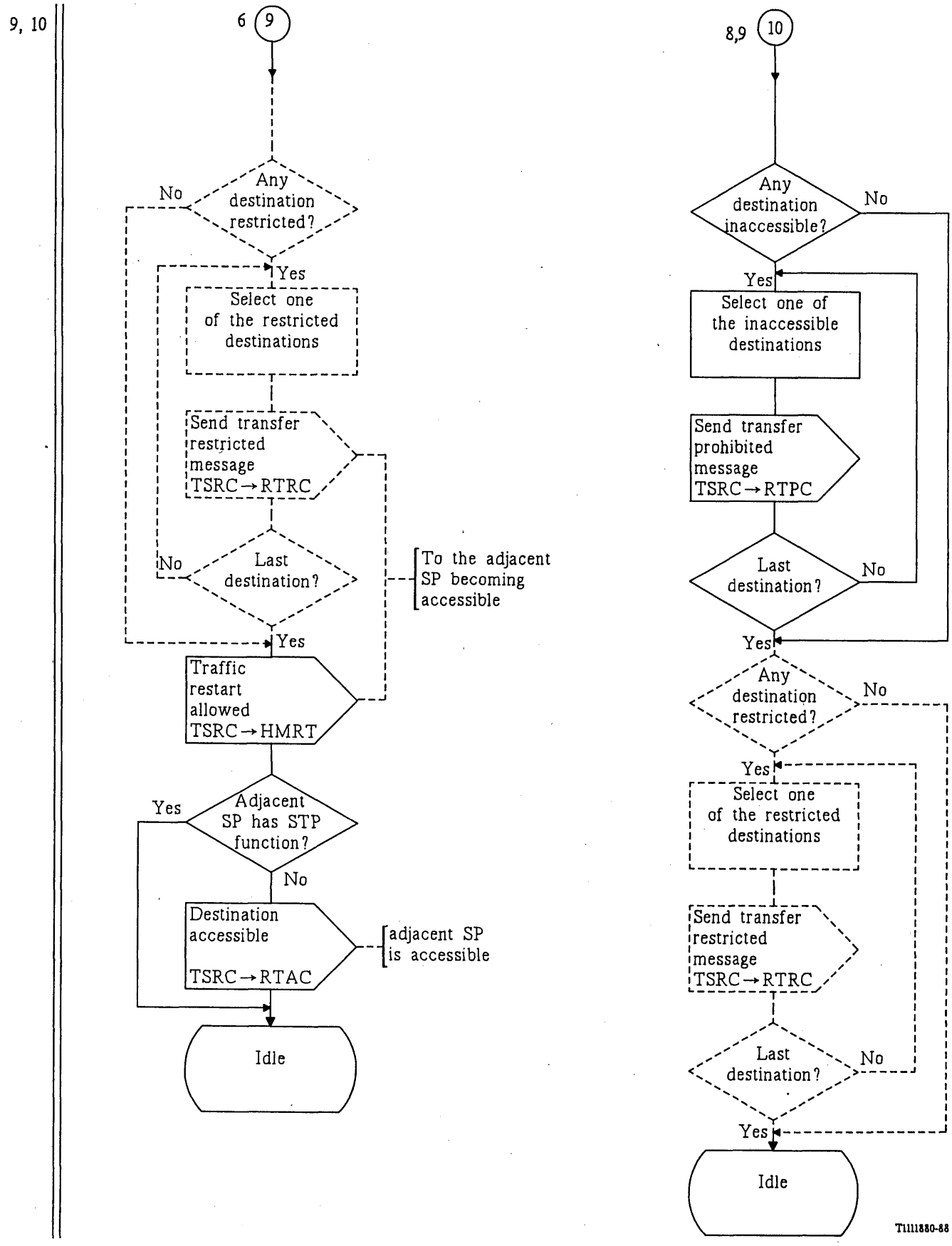



FIGURE 29/Q.704 (Sheet 7 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

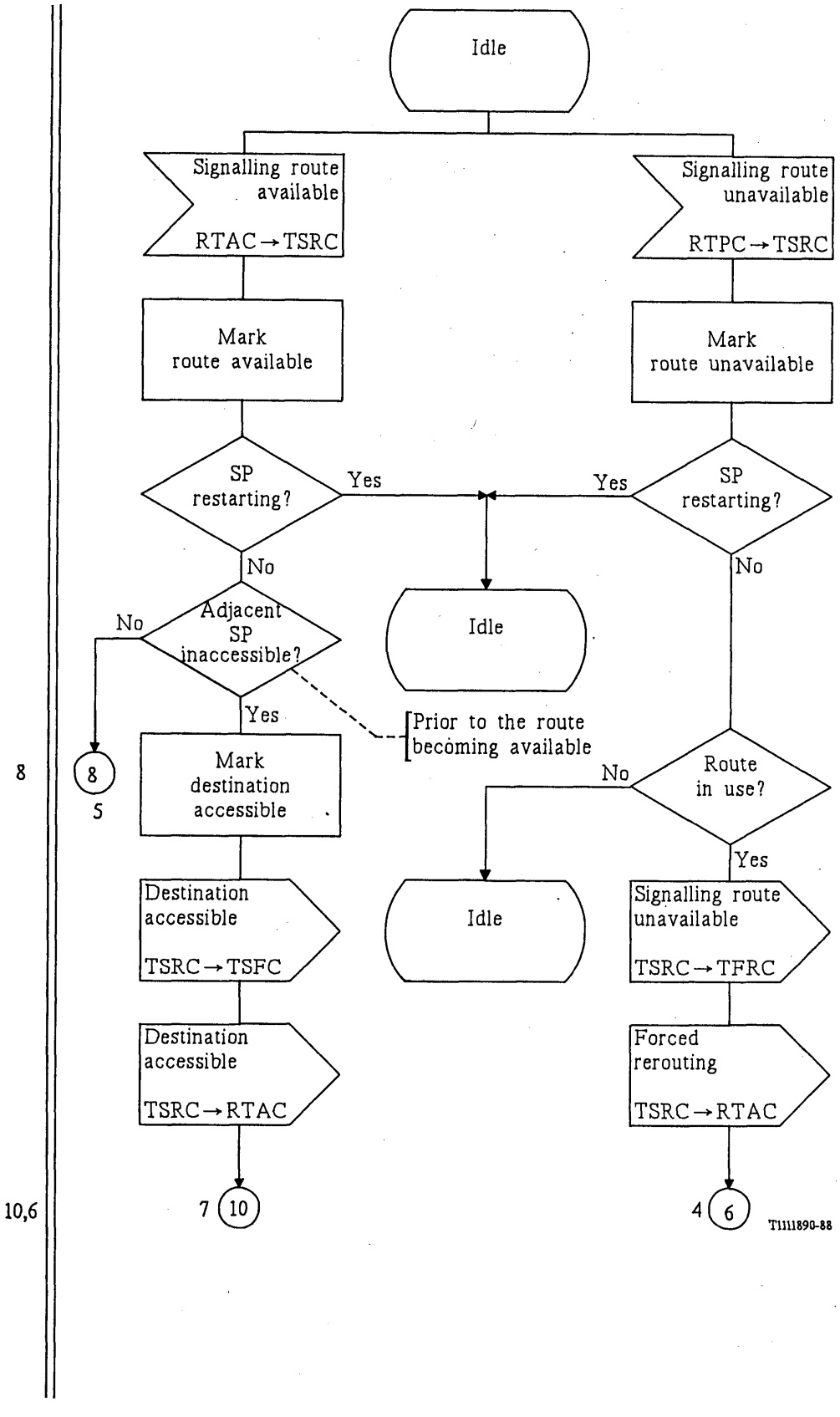
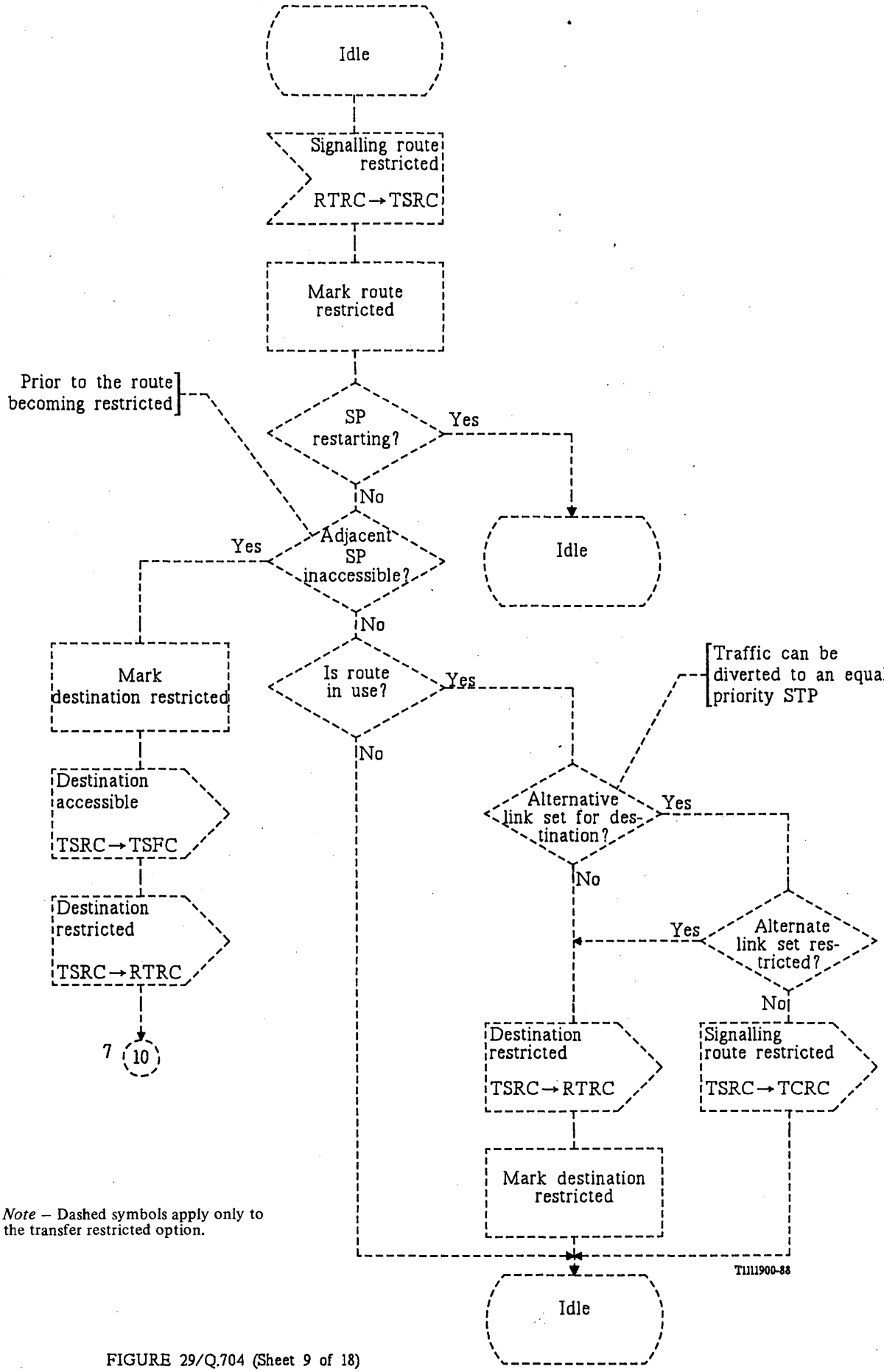



FIGURE 29/Q.704 (Sheet 8 of 18)

Signalling traffic management; signalling routing control (TSRC)




*Note* – Dashed symbols apply only to the transfer restricted option.

FIGURE 29/Q.704 (Sheet 9 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

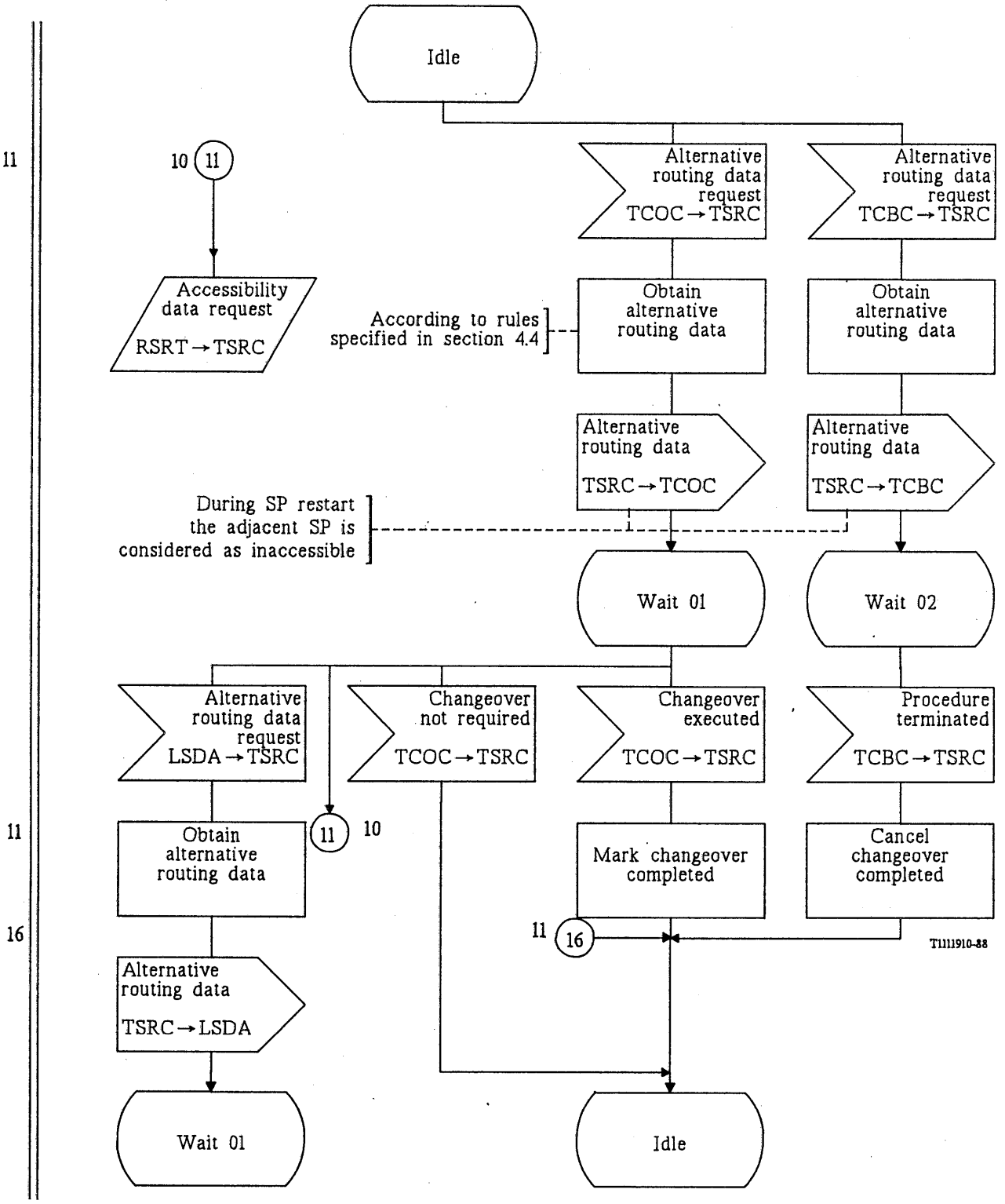



FIGURE 29/Q.704 (Sheet 10 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

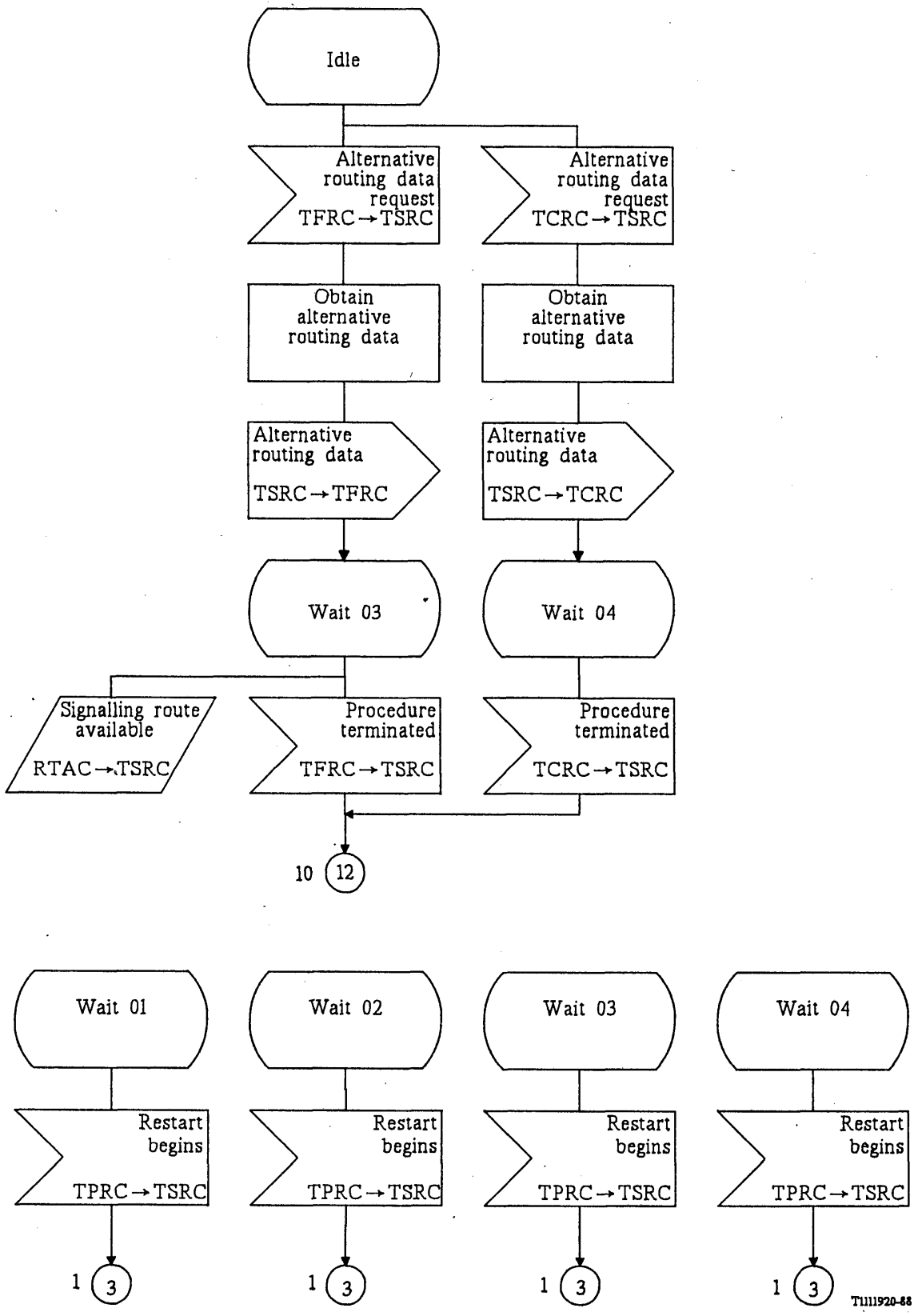
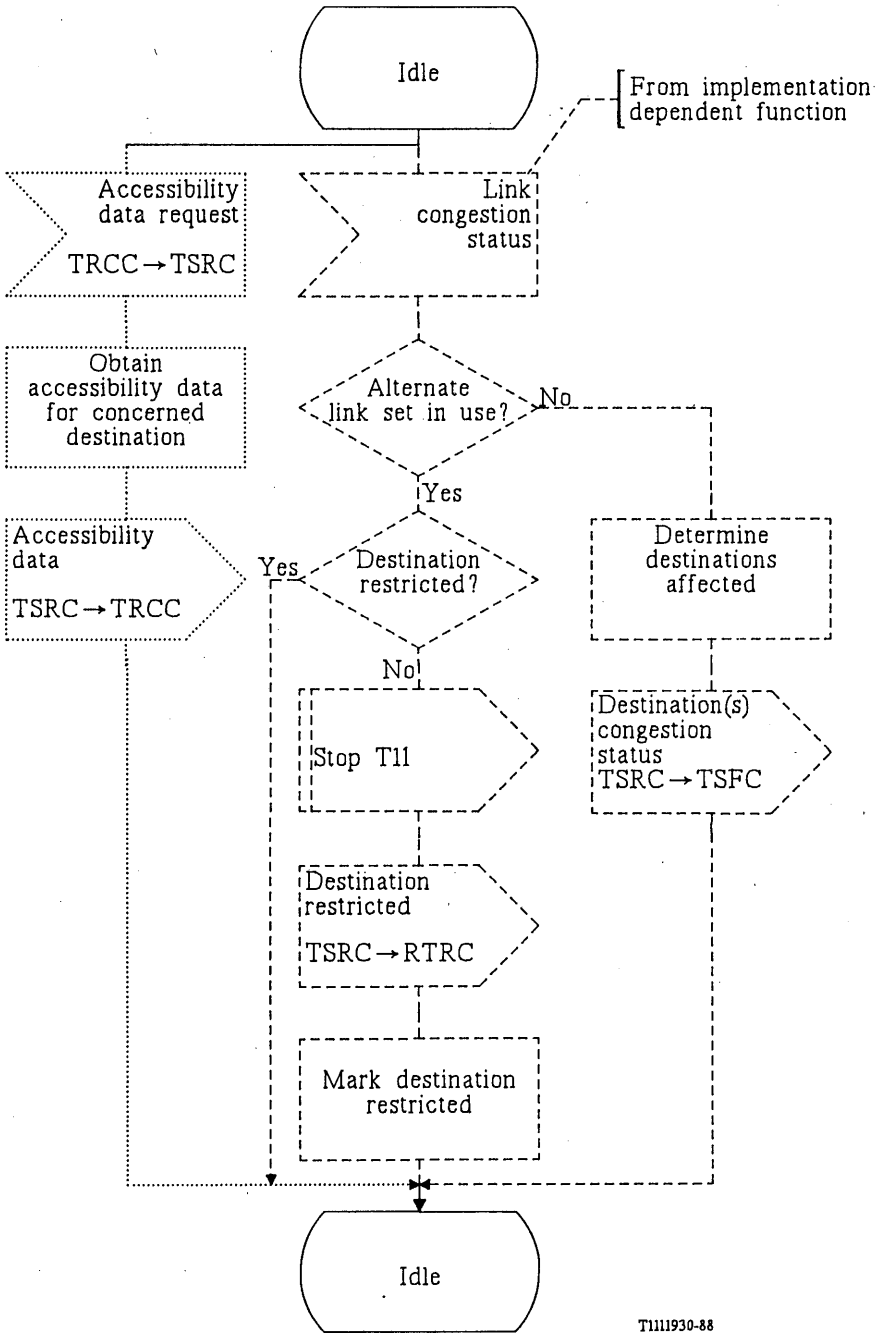



FIGURE 29/Q.704 (Sheet 11 of 18)

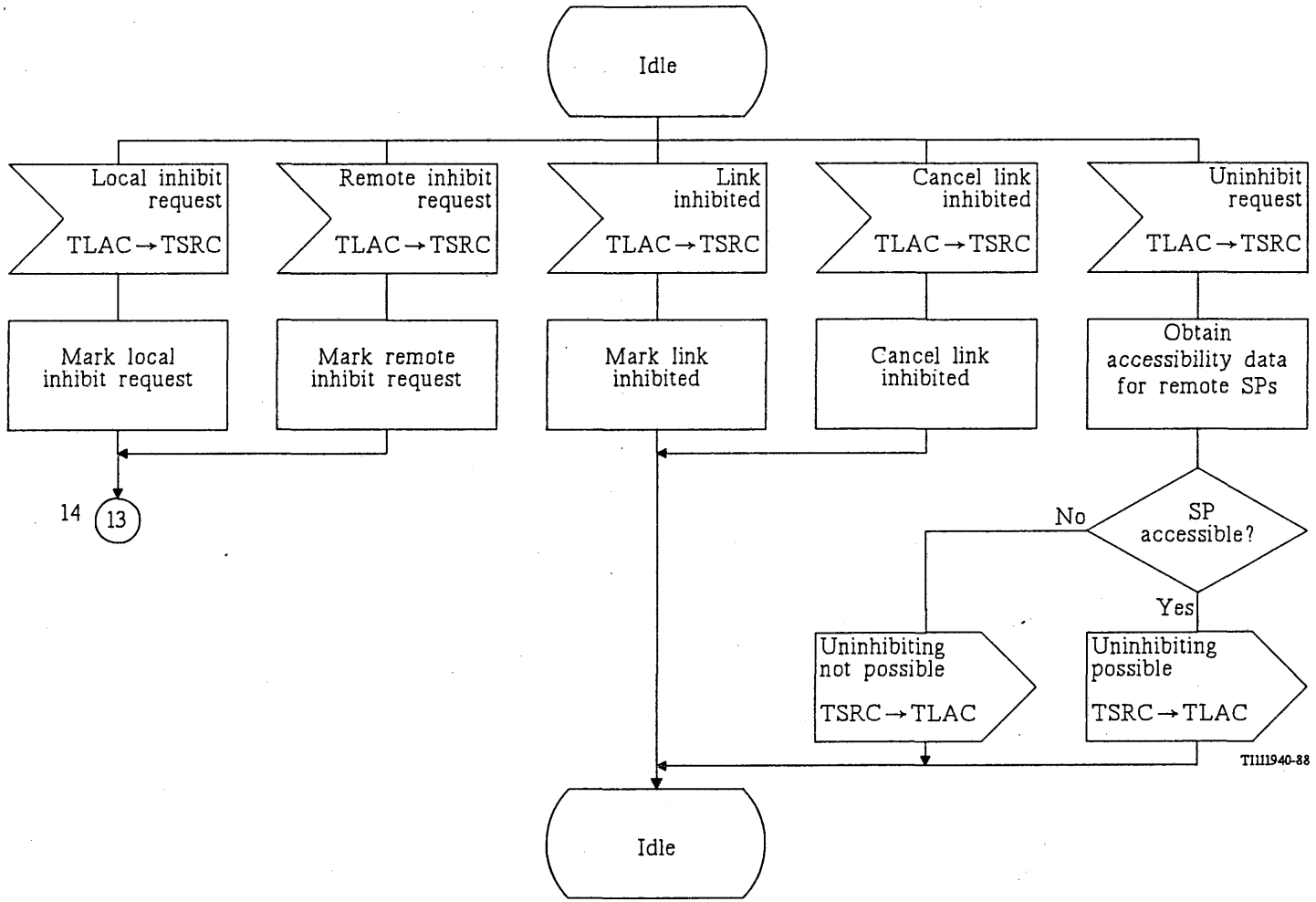
**Signalling traffic management; signalling routing control (TSRC)**




*Note* – Dotted symbols apply only to the multiple congestion states option; dashed symbols apply only to the transfer restricted option.

FIGURE 29/Q.704 (Sheet 12 of 18)

**Signalling traffic management; signalling routing control (TSRC)**




13

FIGURE 29/Q.704 (Sheet 13 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

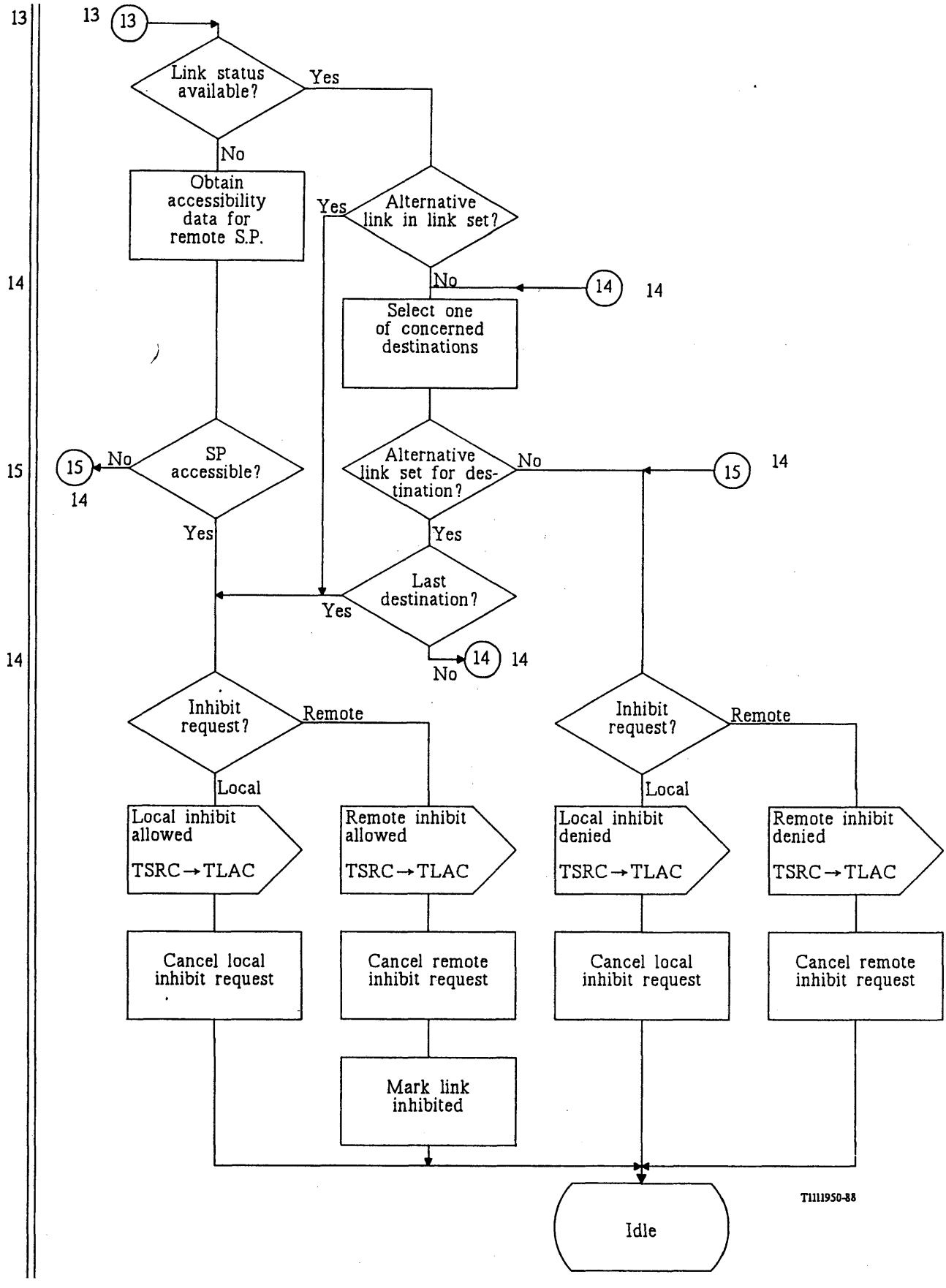
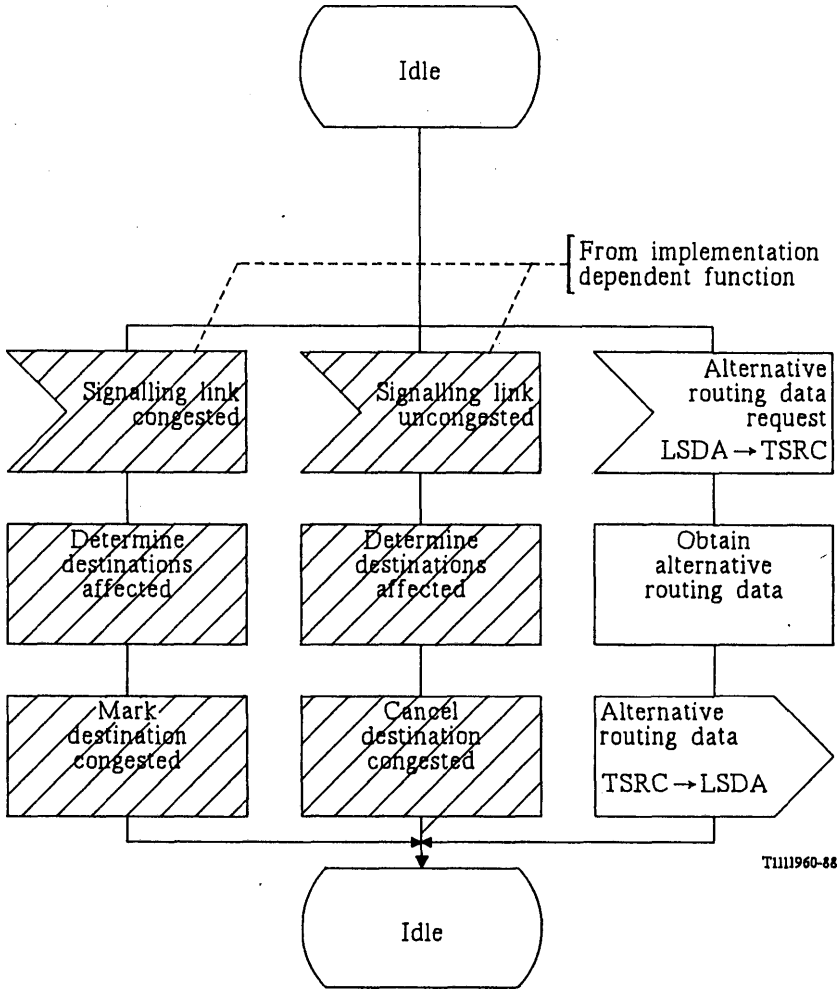



FIGURE 29/Q.704 (Sheet 14 of 18)

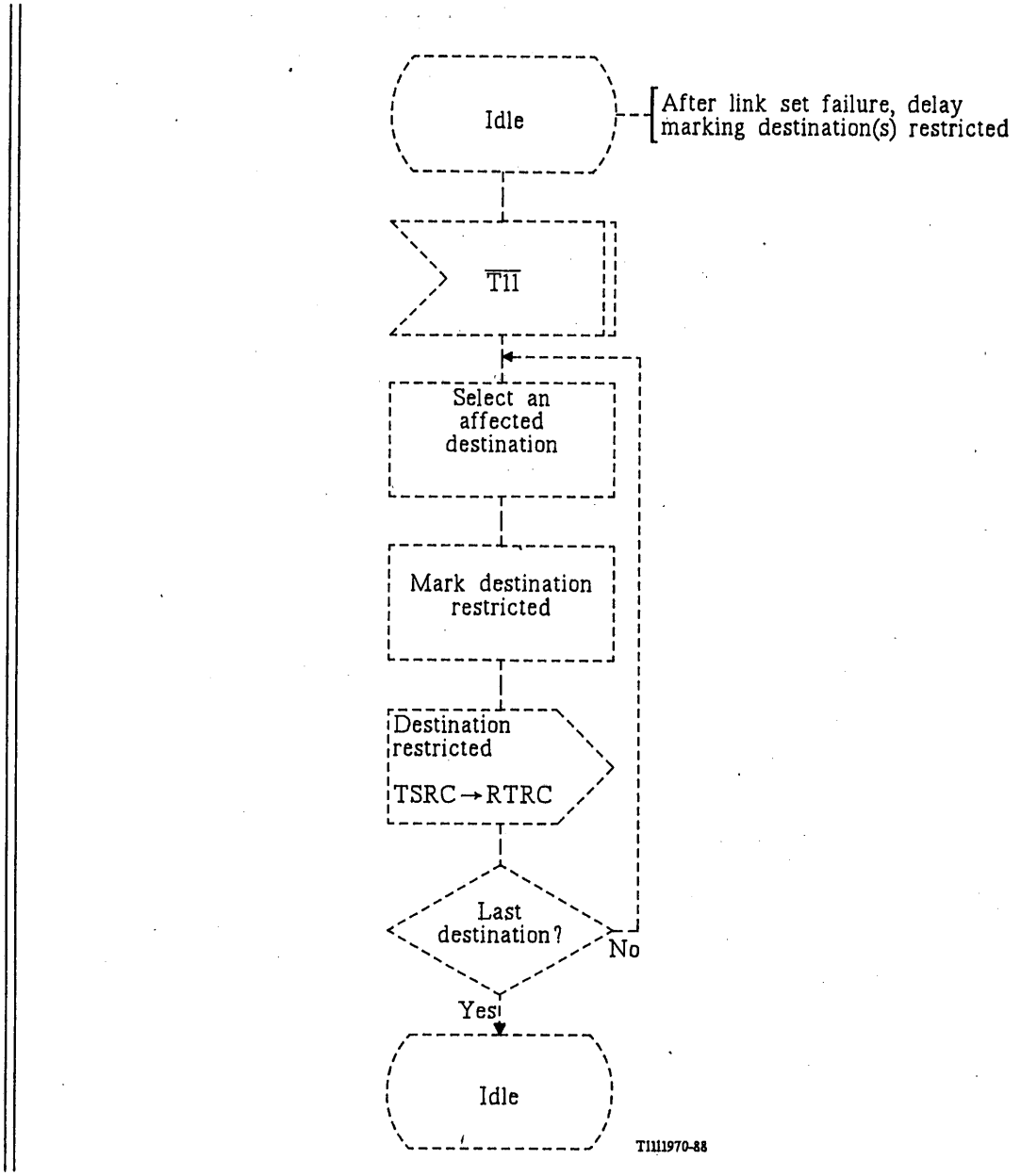
**Signalling traffic management; signalling routing control (TSRC)**




*Note* – Delete hatched symbols when using Multiple Congestion States option.

FIGURE 29/Q.704 (Sheet 15 of 18)

**Signalling traffic management; signalling routing control (TSRC)**




*Note* – Dashed symbols apply only to the transfer restricted option.

FIGURE 29/Q.704 (Sheet 16 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

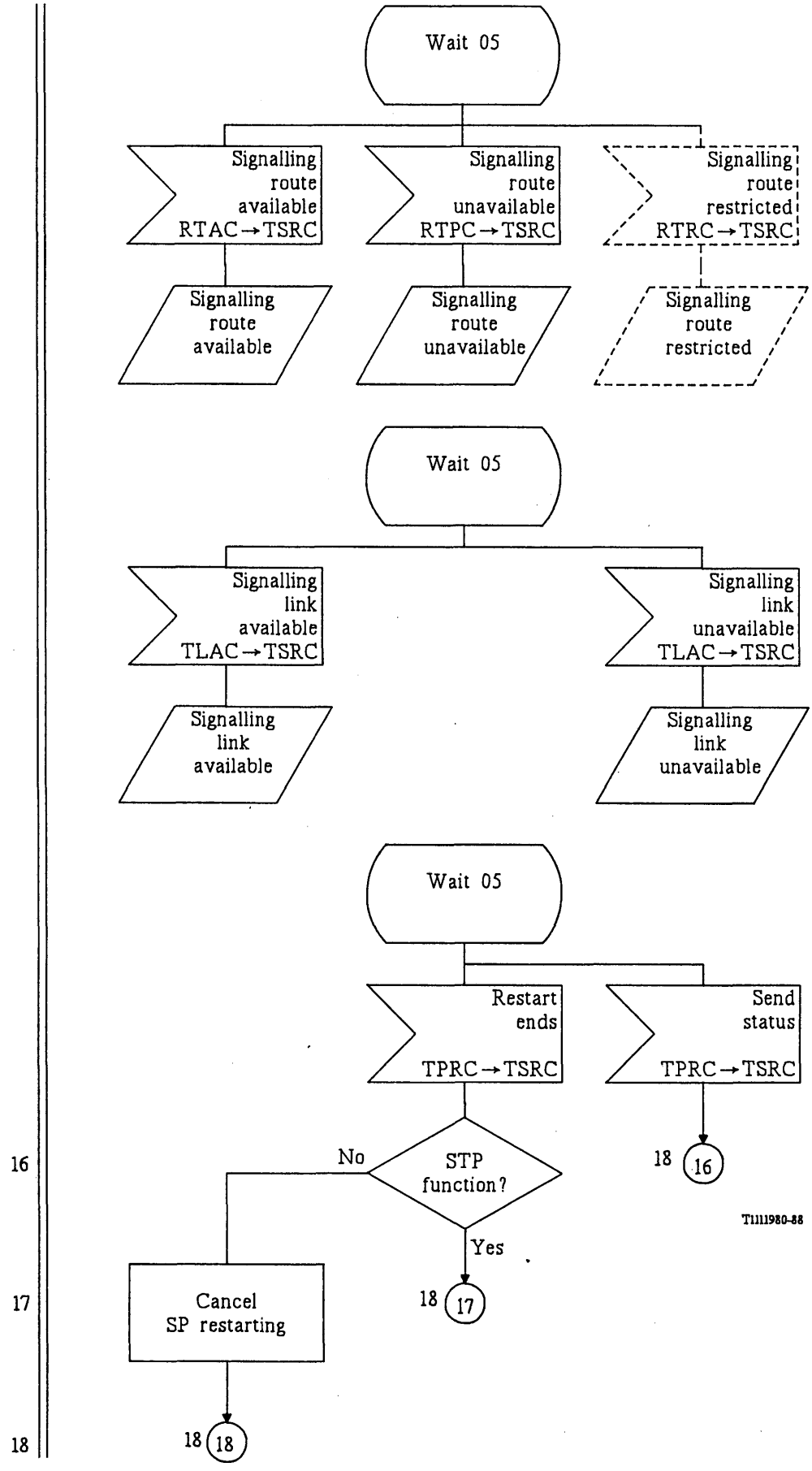



FIGURE 29/Q.704 (Sheet 17 of 18)

**Signalling traffic management; signalling routing control (TSRC)**

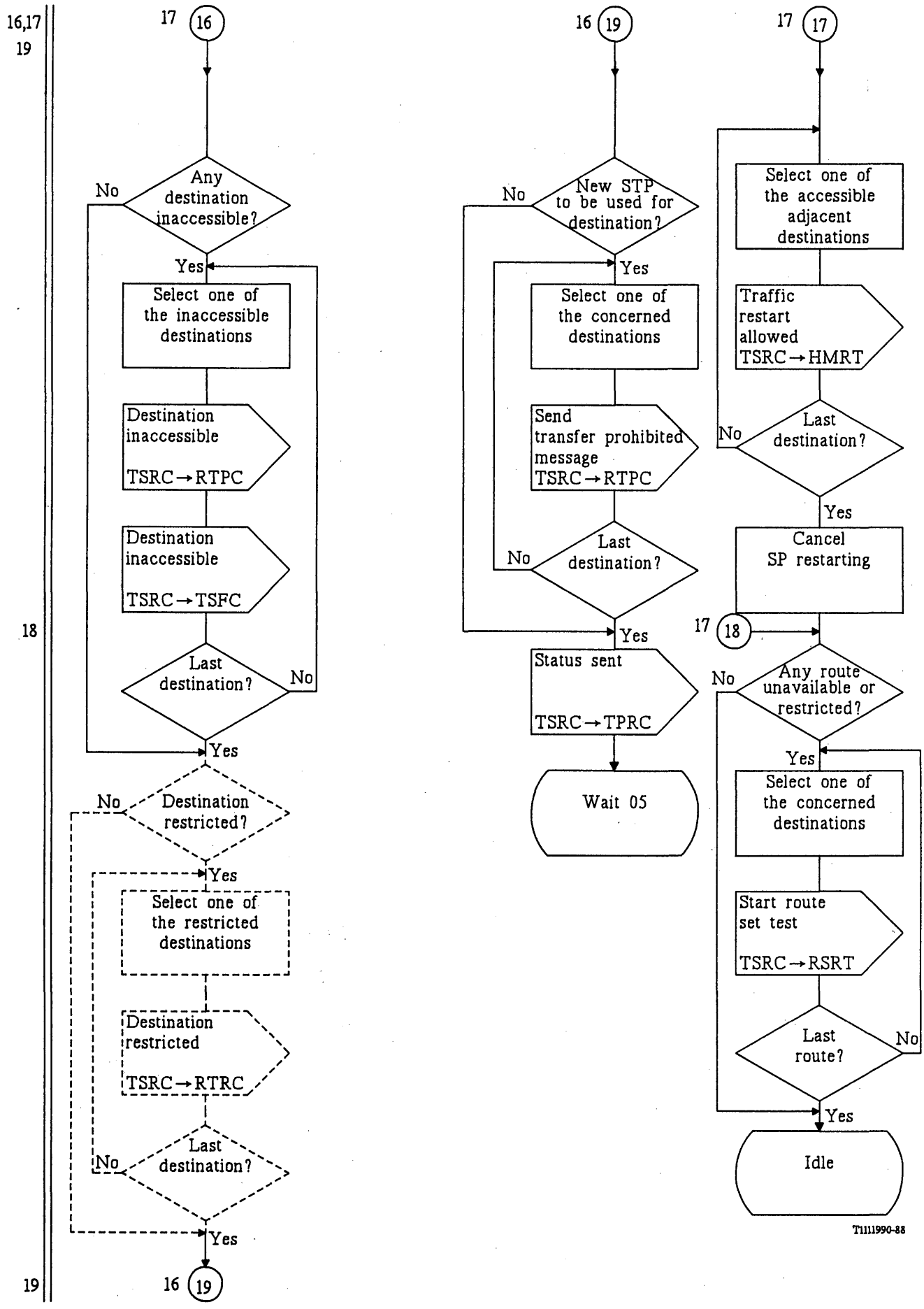
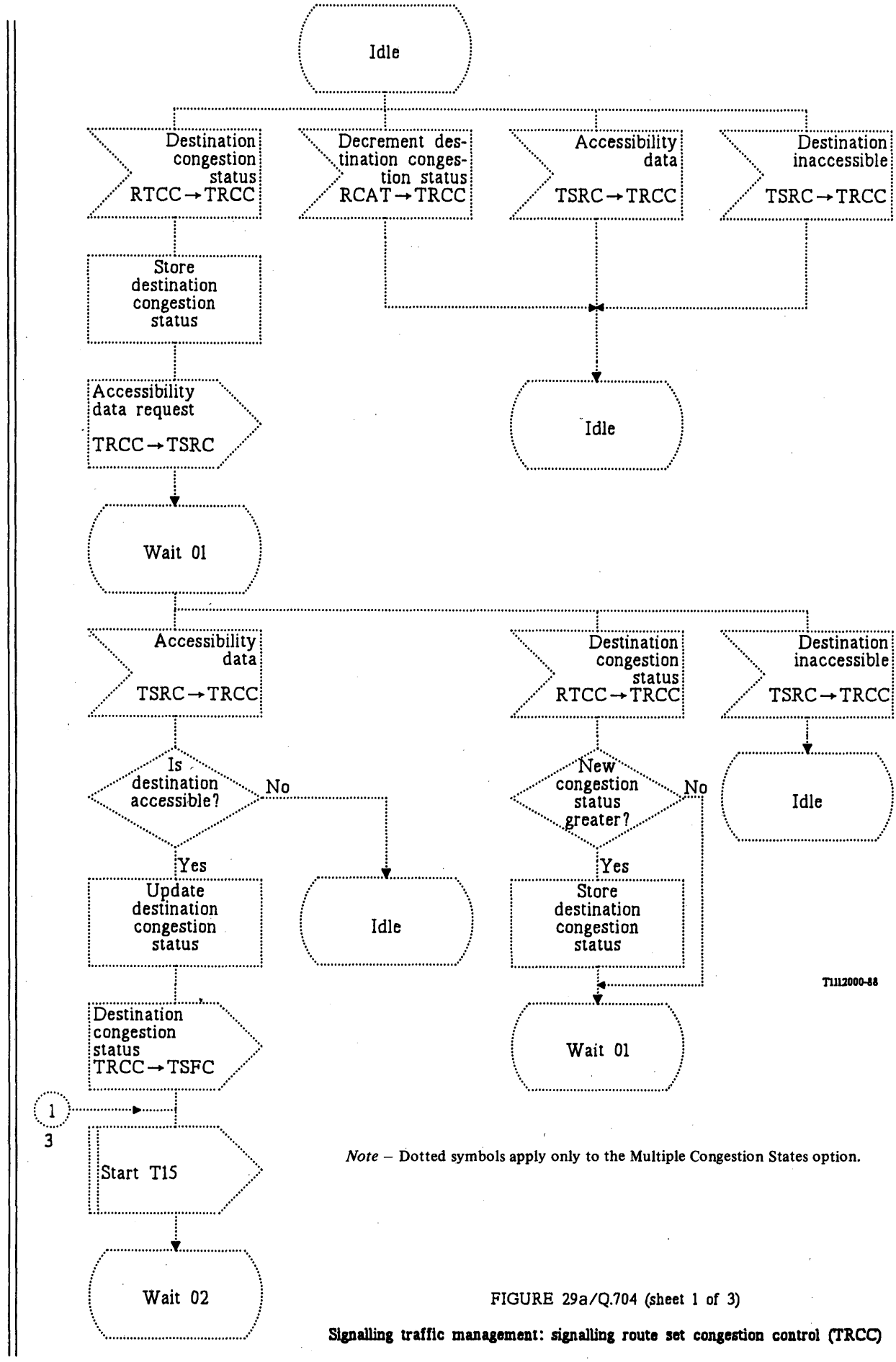



FIGURE 29/Q.704 (Sheet 18 of 18)

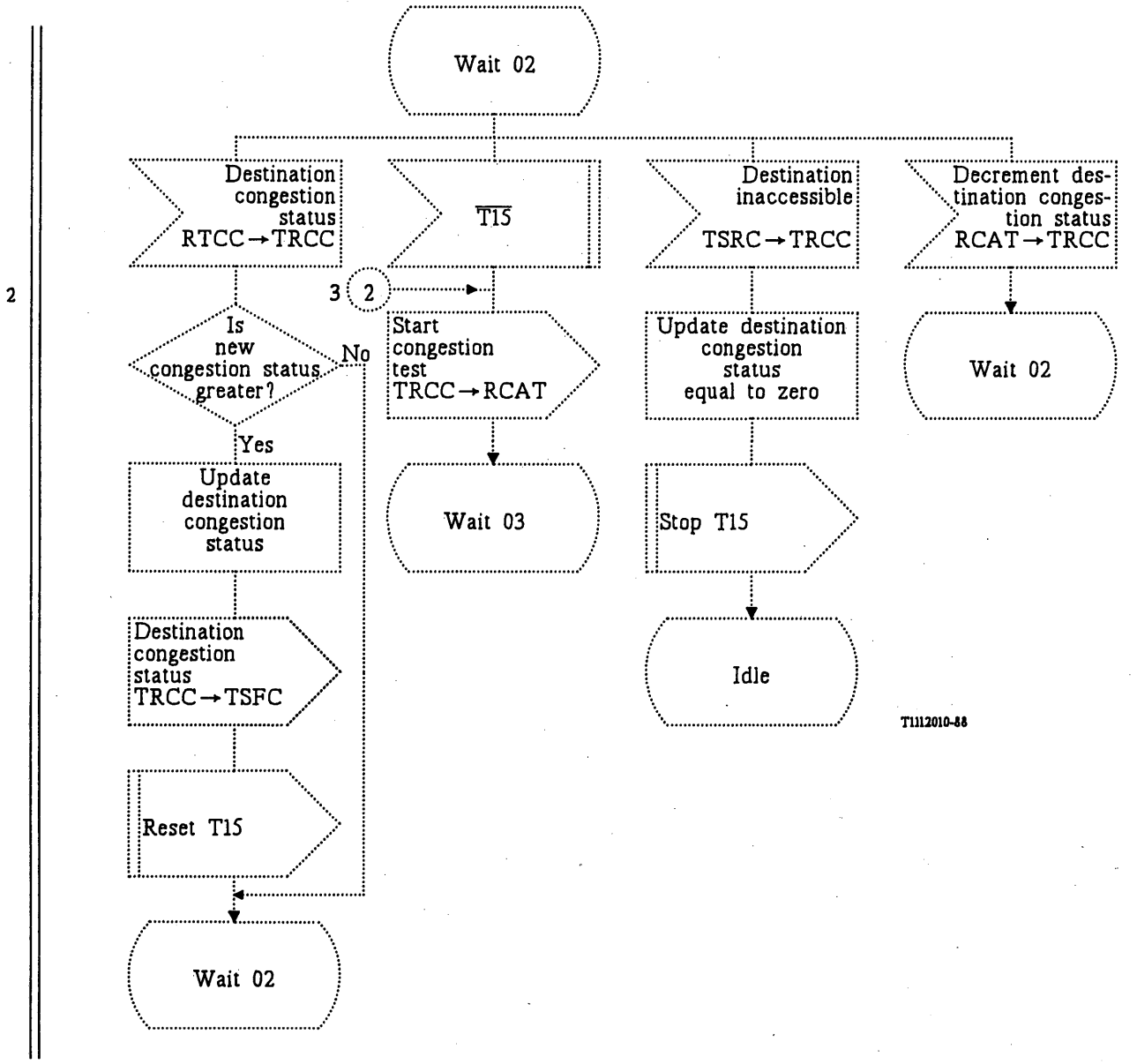
**Signalling traffic management; signalling routing control (TSRC)**




*Note* – Dotted symbols apply only to the Multiple Congestion States option.

FIGURE 29a/Q.704 (sheet 1 of 3)

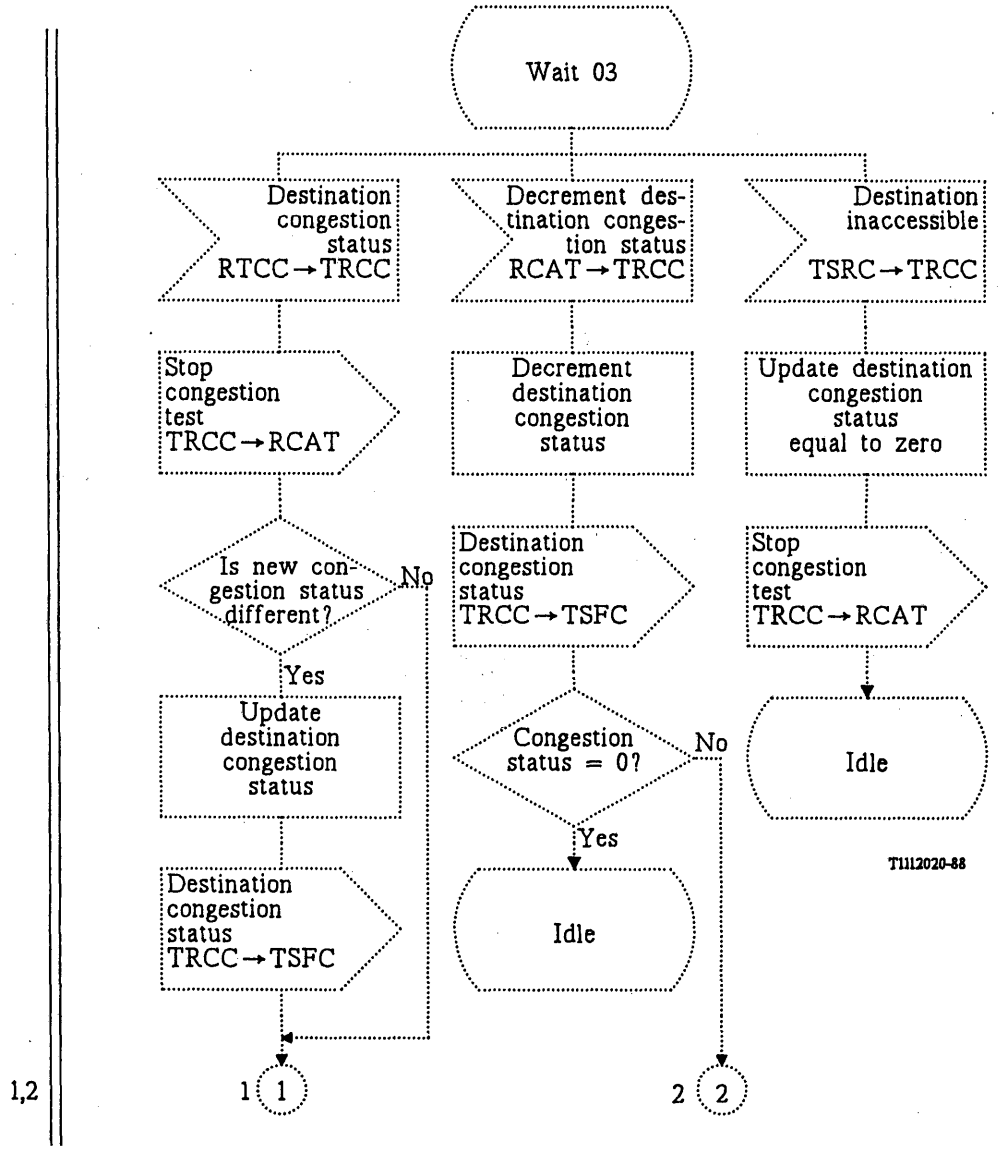
**Signalling traffic management: signalling route set congestion control (TRCC)**




*Note* – Dotted symbols apply only to the Multiple Congestion States option.

FIGURE 29a/Q.704 (Sheet 2 of 3)

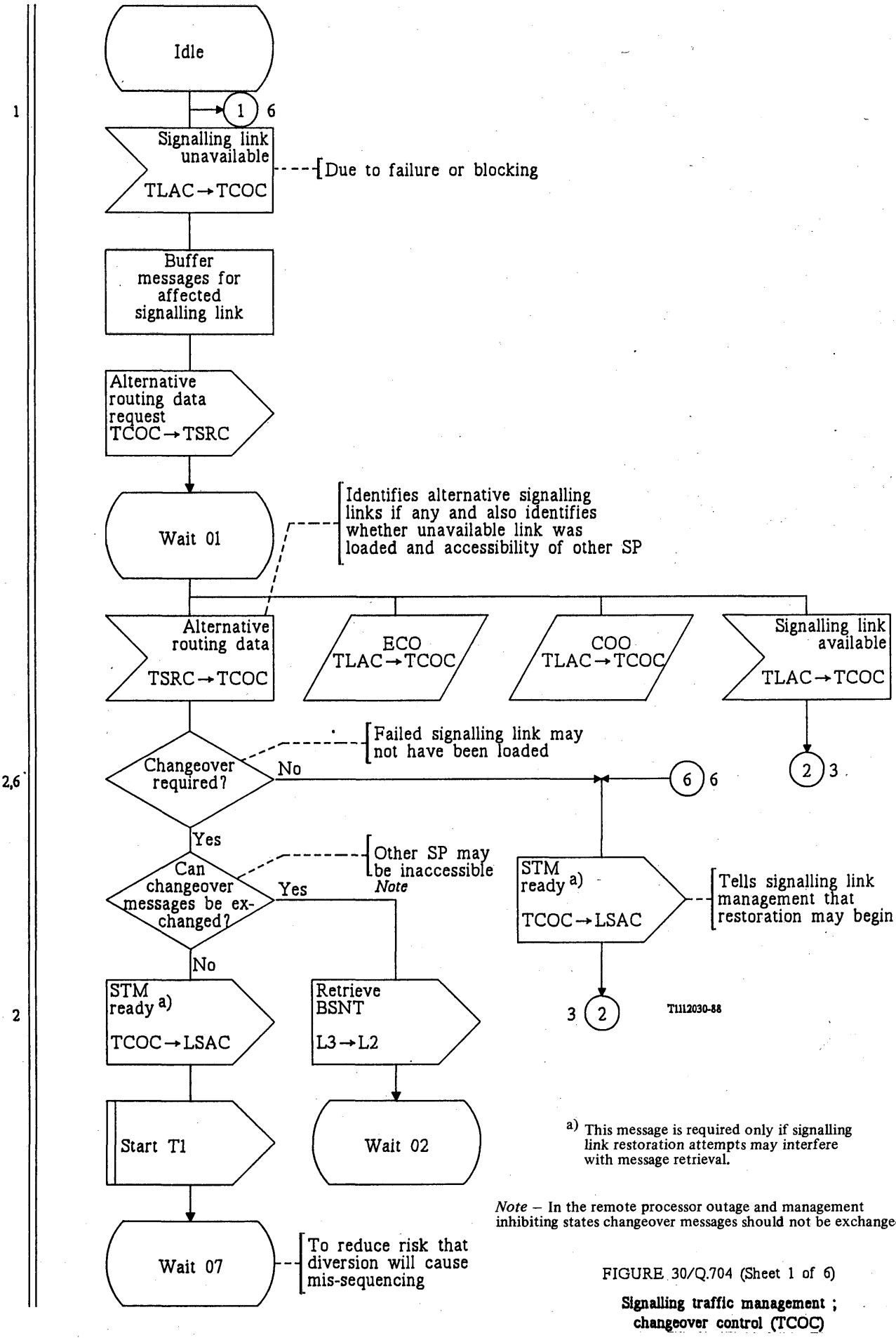
**Signalling traffic management: signalling route set congestion control (TRCC)**




*Note* – Dotted symbols apply only to the Multiple Congestion States option.

FIGURE 29a/Q.704 (Sheet 3 of 3)

**Signalling traffic management: signalling route set congestion control (TRCC)**




a) This message is required only if signalling link restoration attempts may interfere with message retrieval.

*Note* – In the remote processor outage and management inhibiting states changeover messages should not be exchanged.

FIGURE 30/Q.704 (Sheet 1 of 6)

**Signalling traffic management ; changeover control (TCOC)**

2

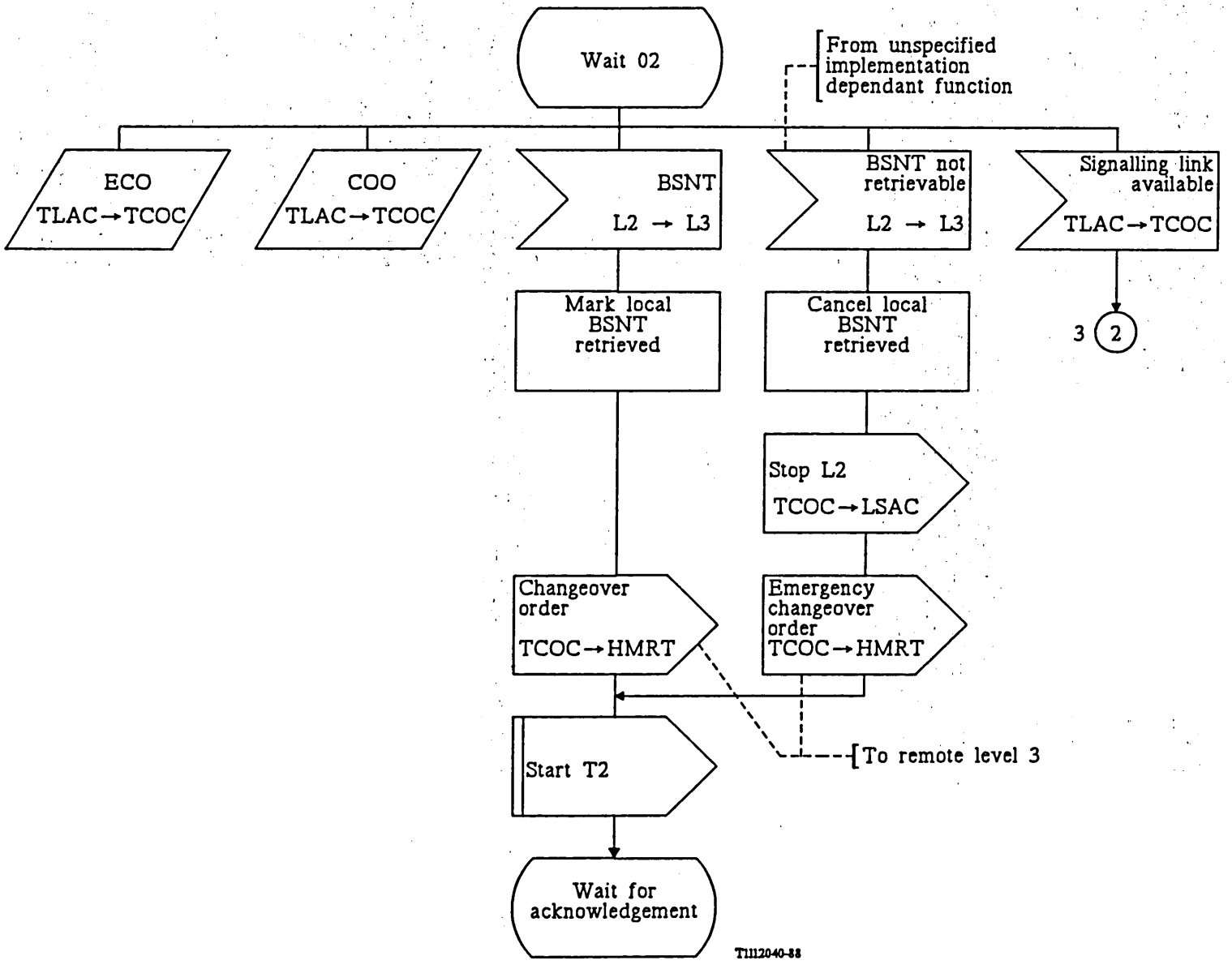
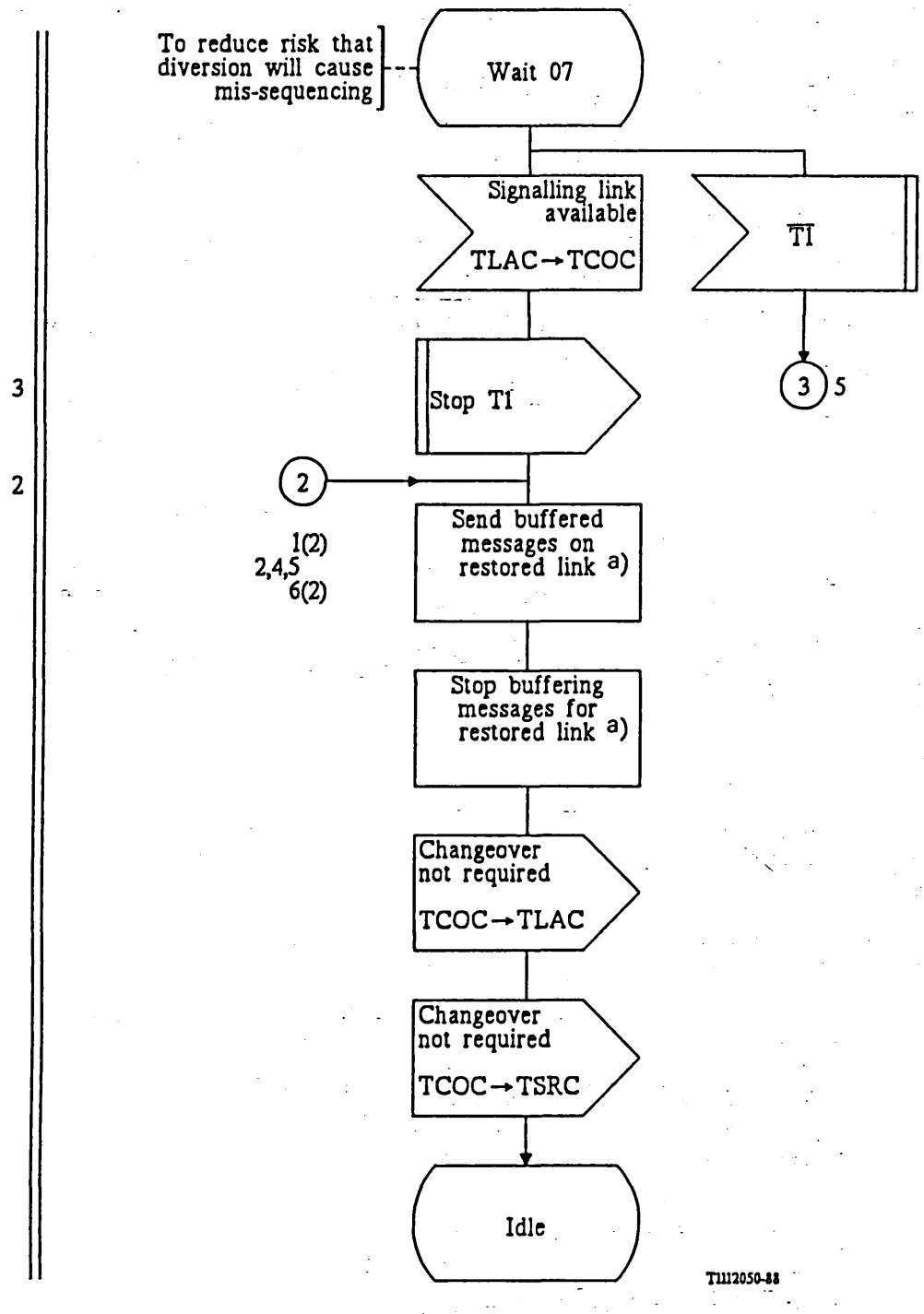



FIGURE 30/Q.704 (Sheet 2 of 6)

**Signalling traffic management; changeover control (TCOC)**




a) These tasks should be carried out in the order shown.

FIGURE 30/Q.704 (Sheet 3 of 6)

**Signalling traffic management; changeover control (TCOC)**

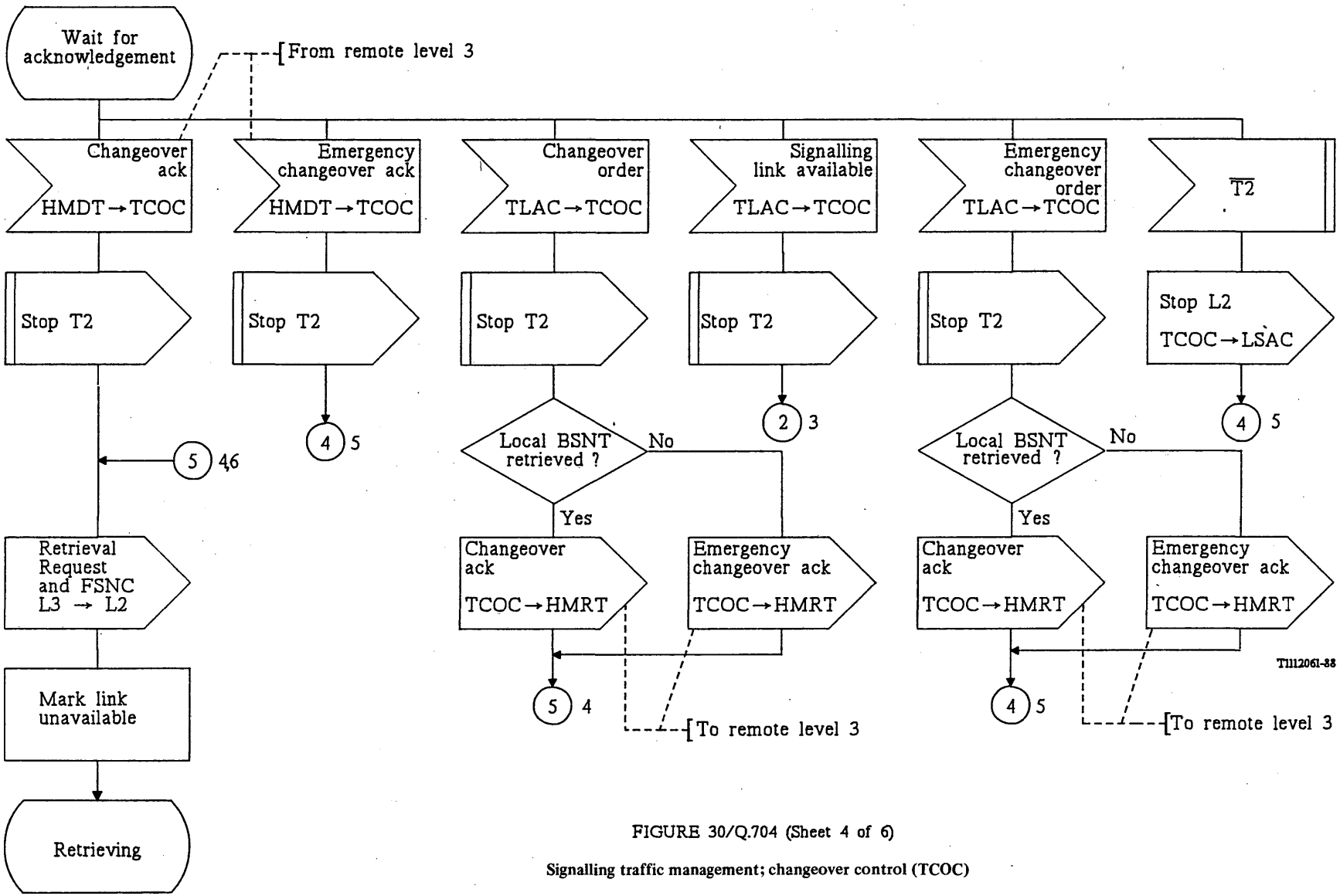



FIGURE 30/Q.704 (Sheet 4 of 6)

**Signalling traffic management; changeover control (TCOC)**

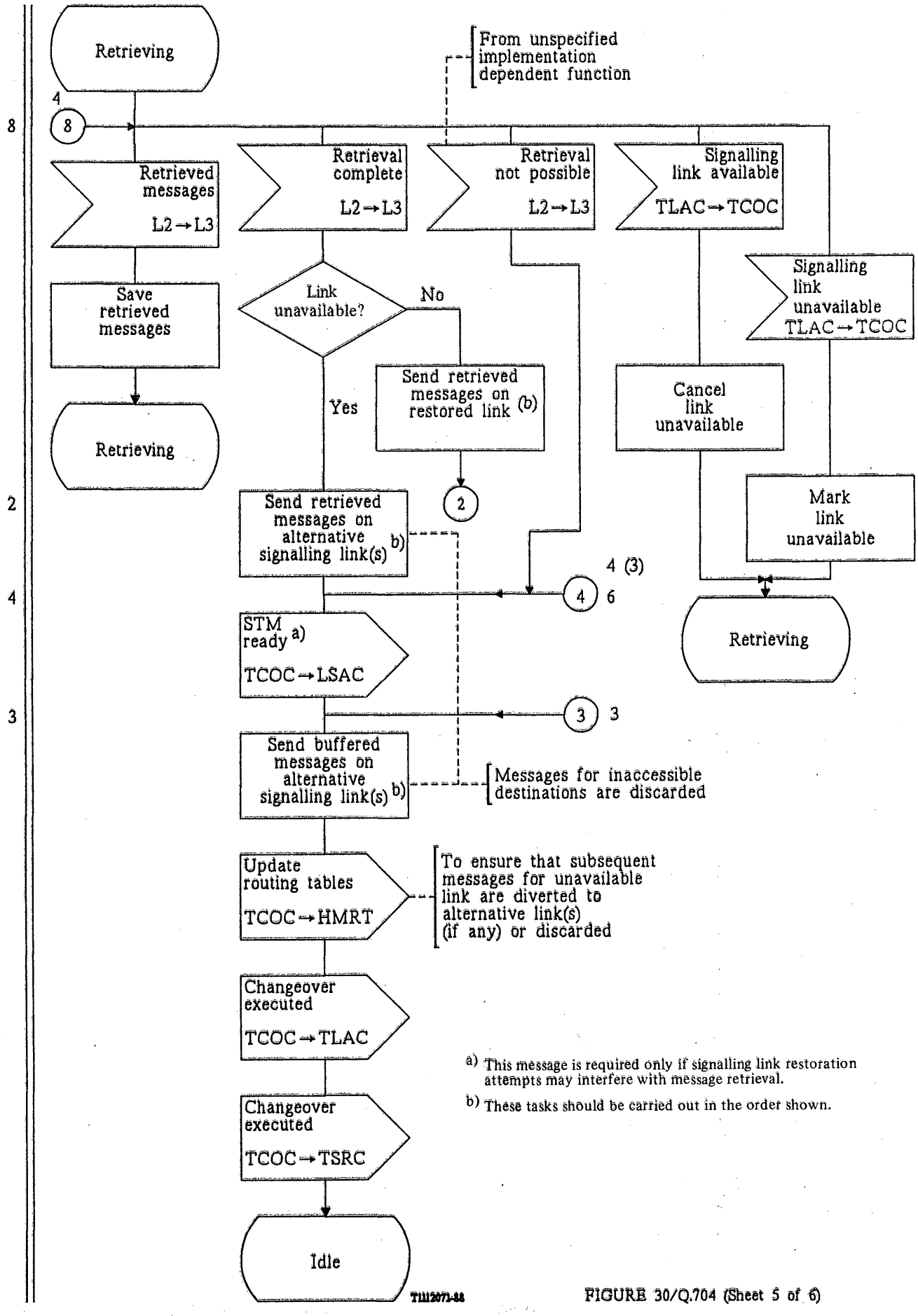



FIGURE 30/Q.704 (Sheet 5 of 6)

**Signalling traffic management; changeover control (TCOC)**

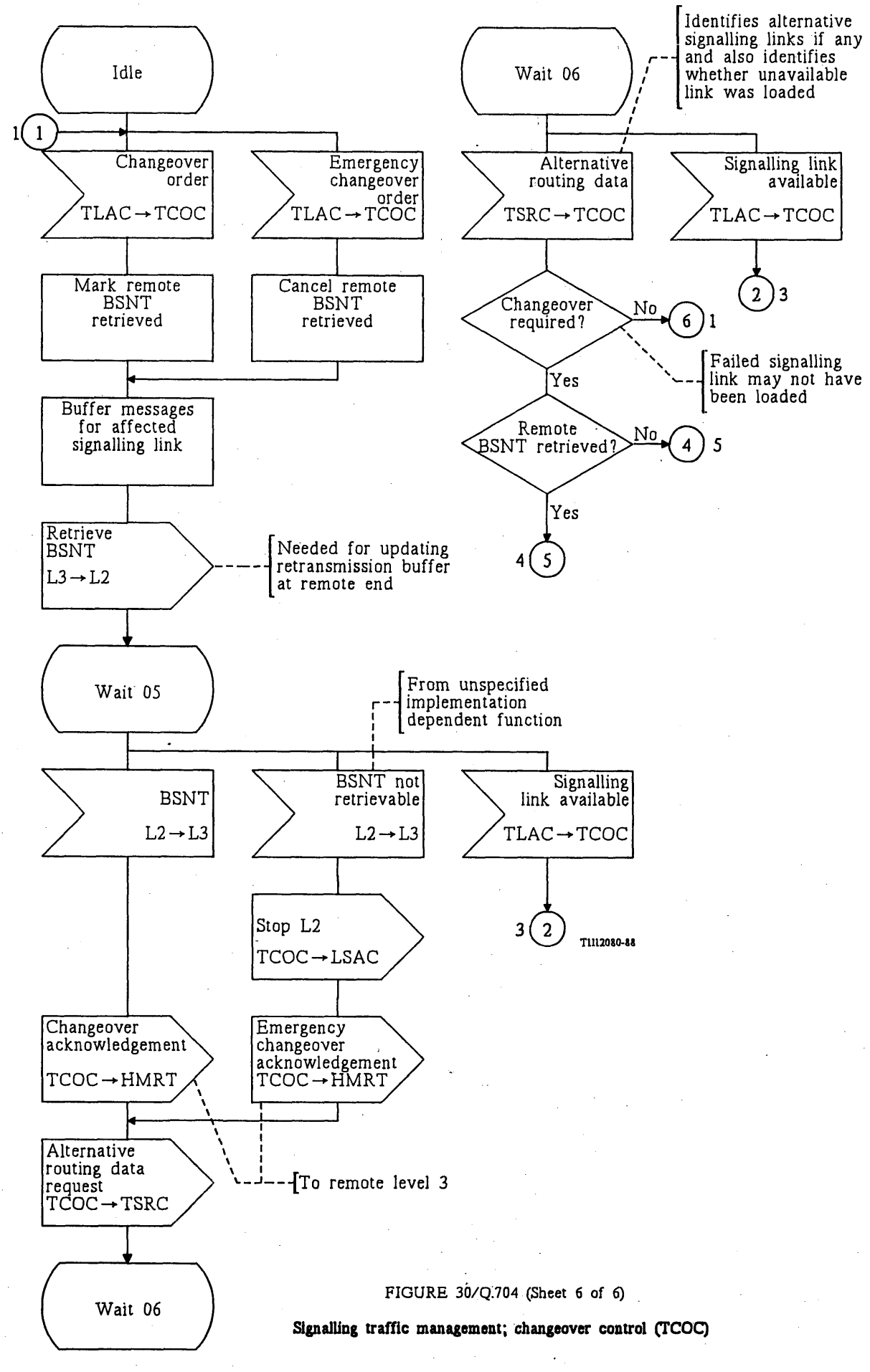



FIGURE 30/Q.704 (Sheet 6 of 6)

**Signalling traffic management; changeover control (TCOC)**

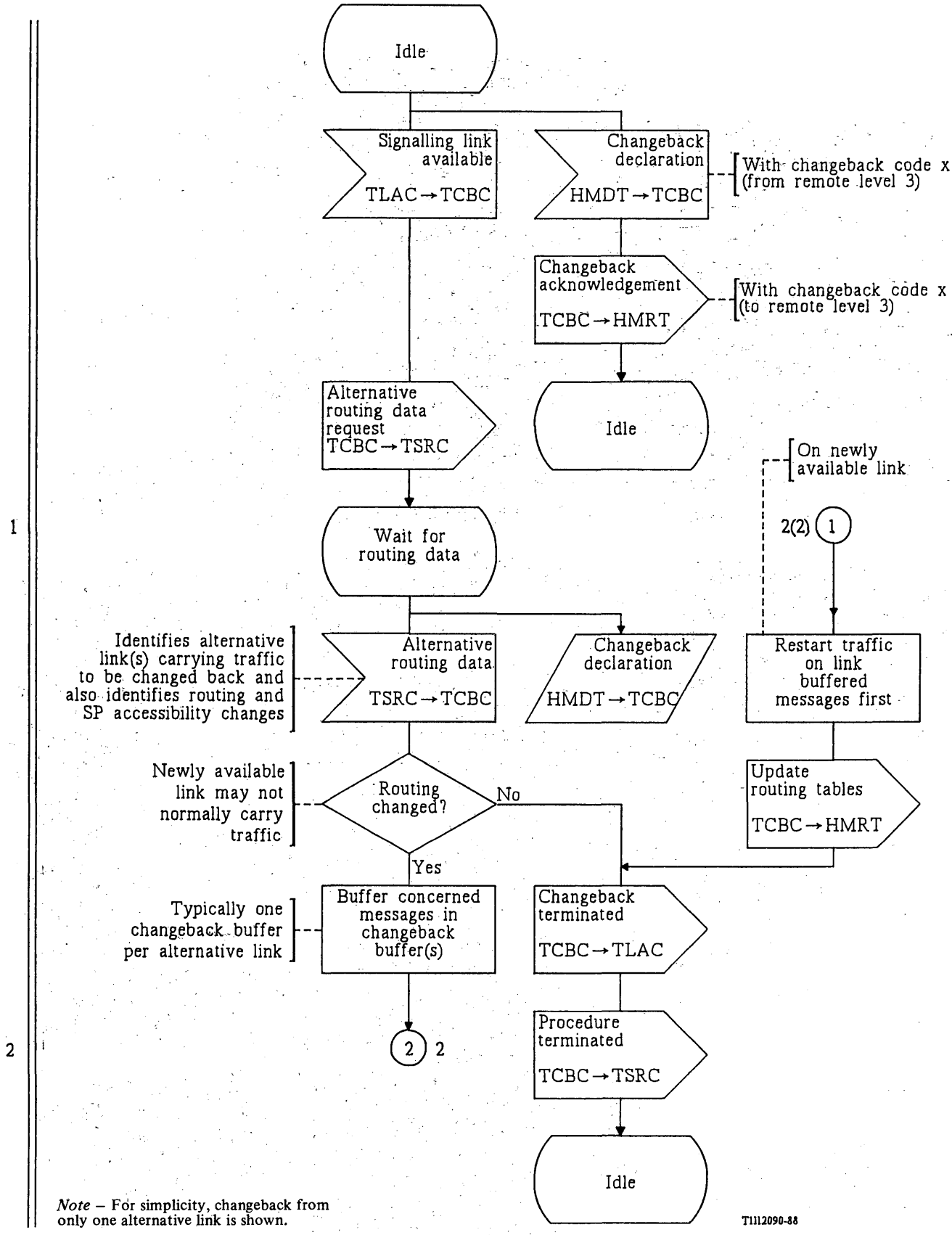



FIGURE 31/Q.704 (Sheet 1 of 2)

**Signalling traffic management; changeback control (TCBC)**

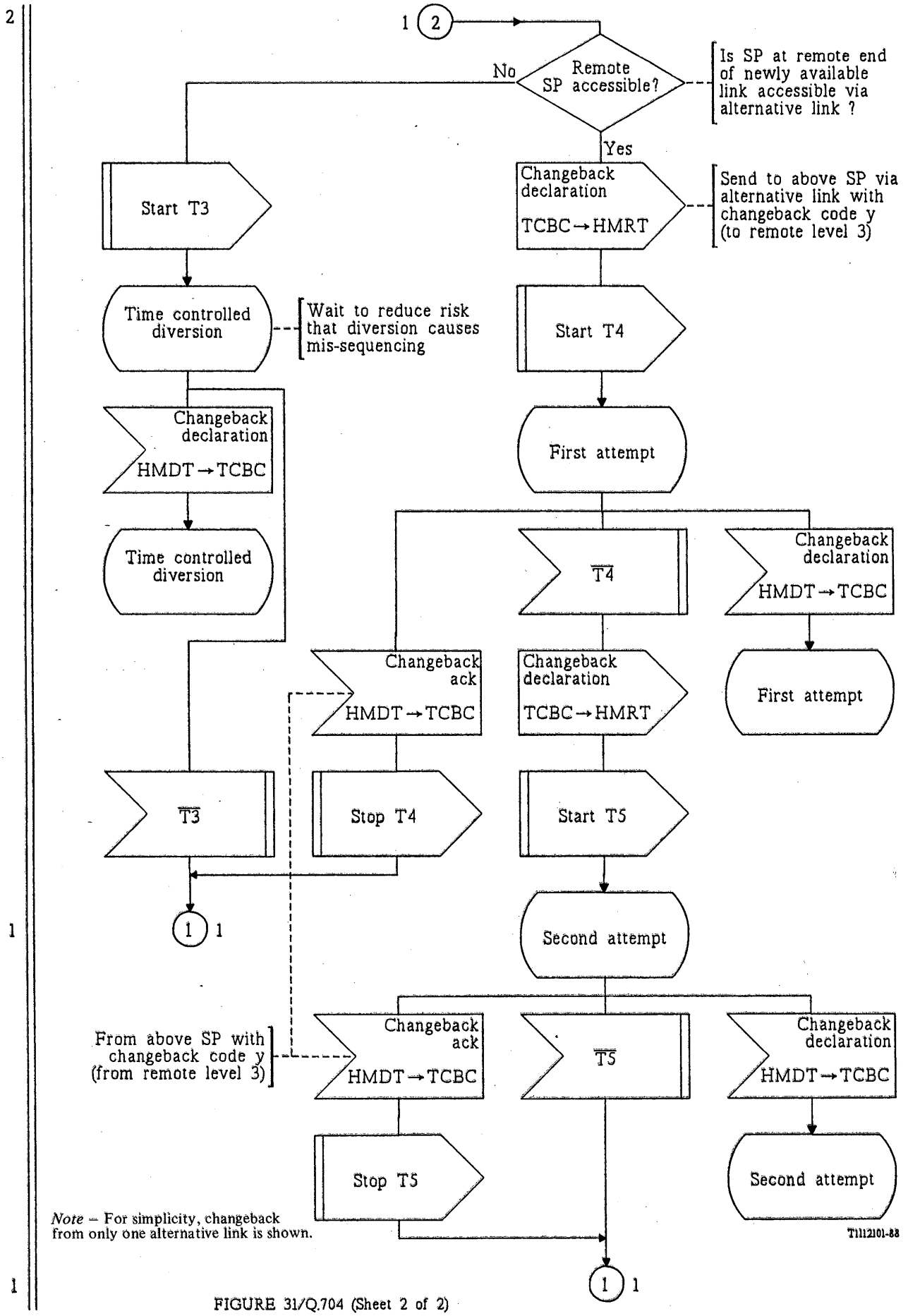



FIGURE 31/Q.704 (Sheet 2 of 2)

**Signalling traffic management; changeback control (TCBC)**

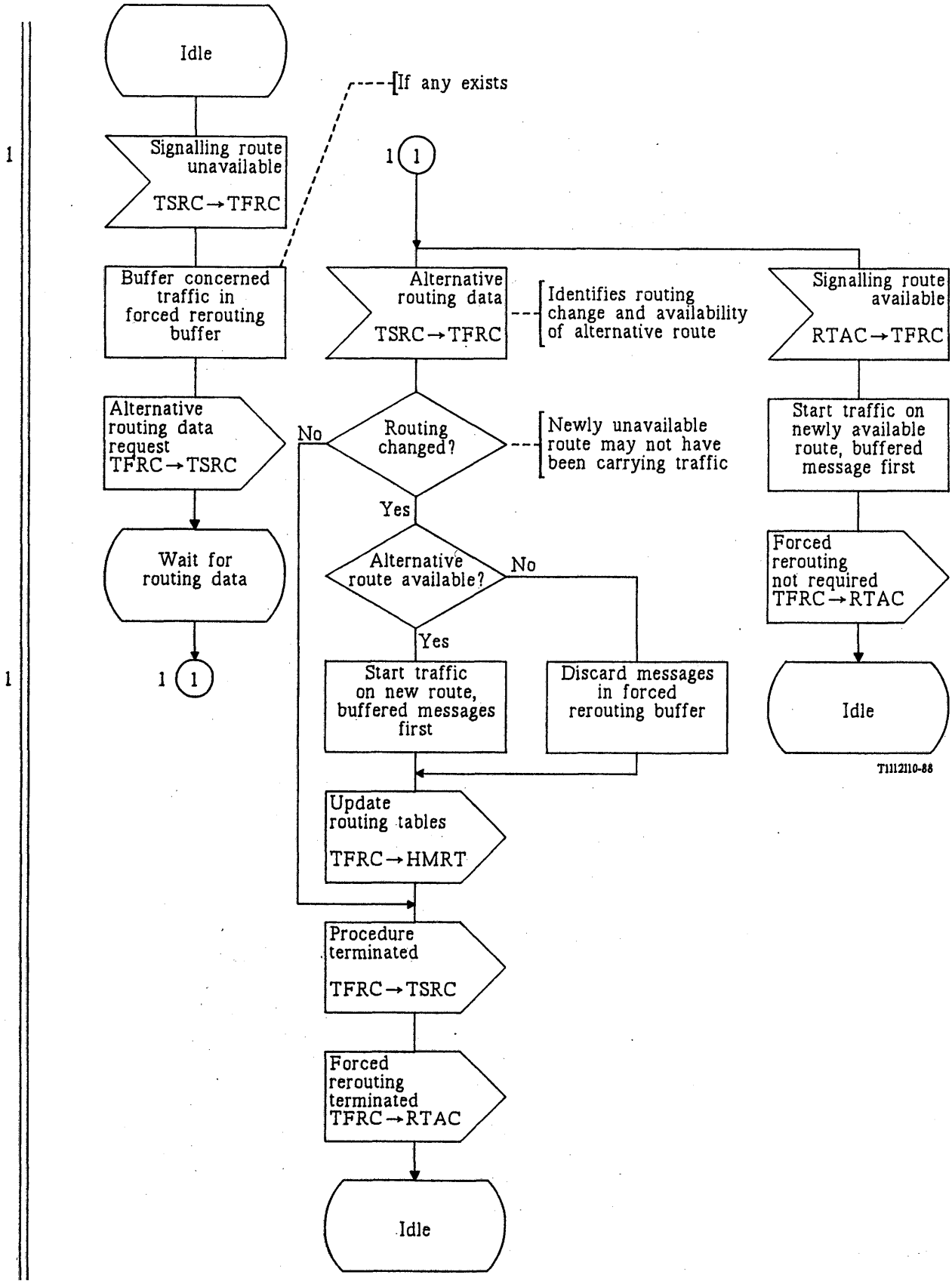
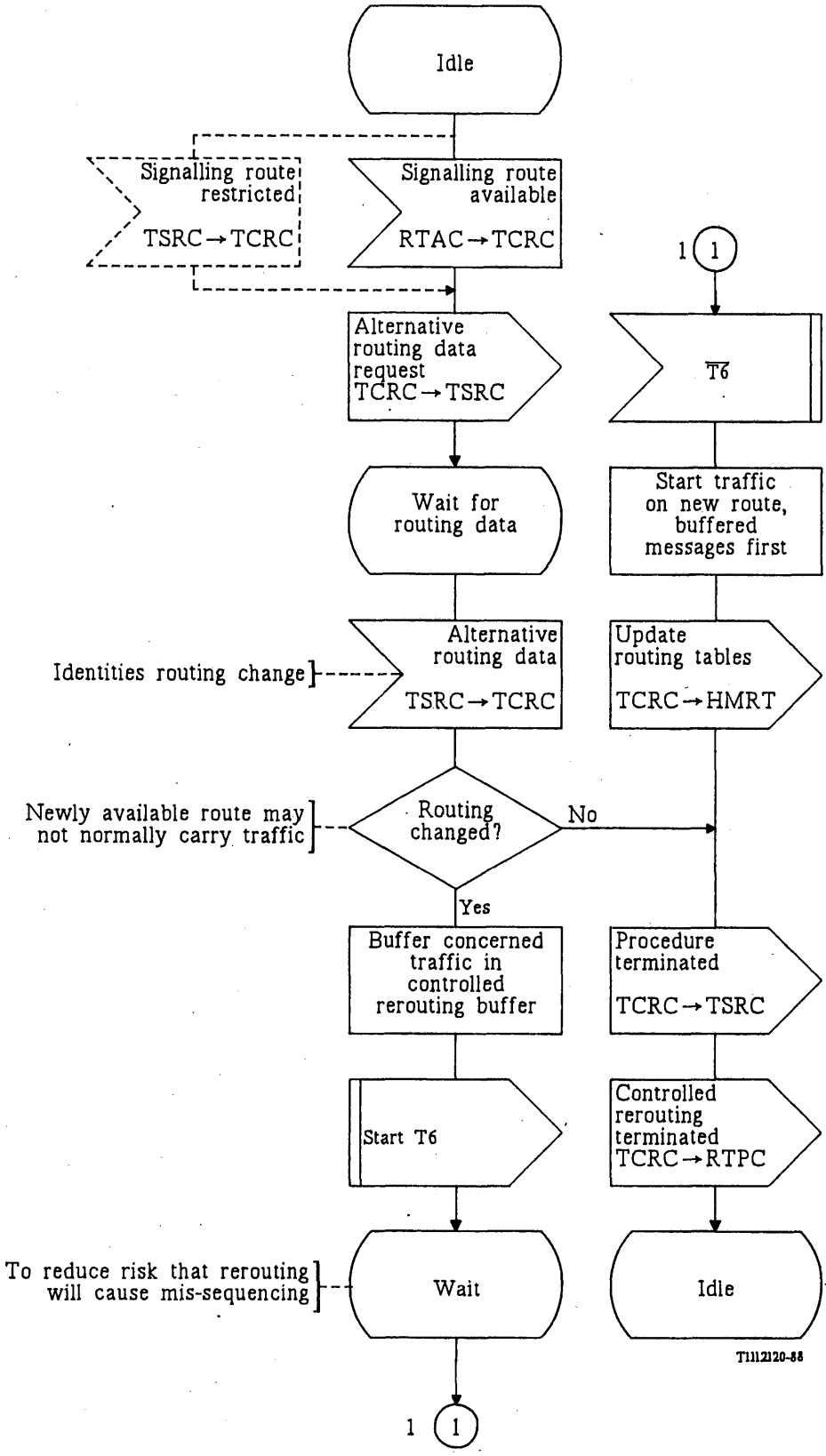



FIGURE 32/Q.704

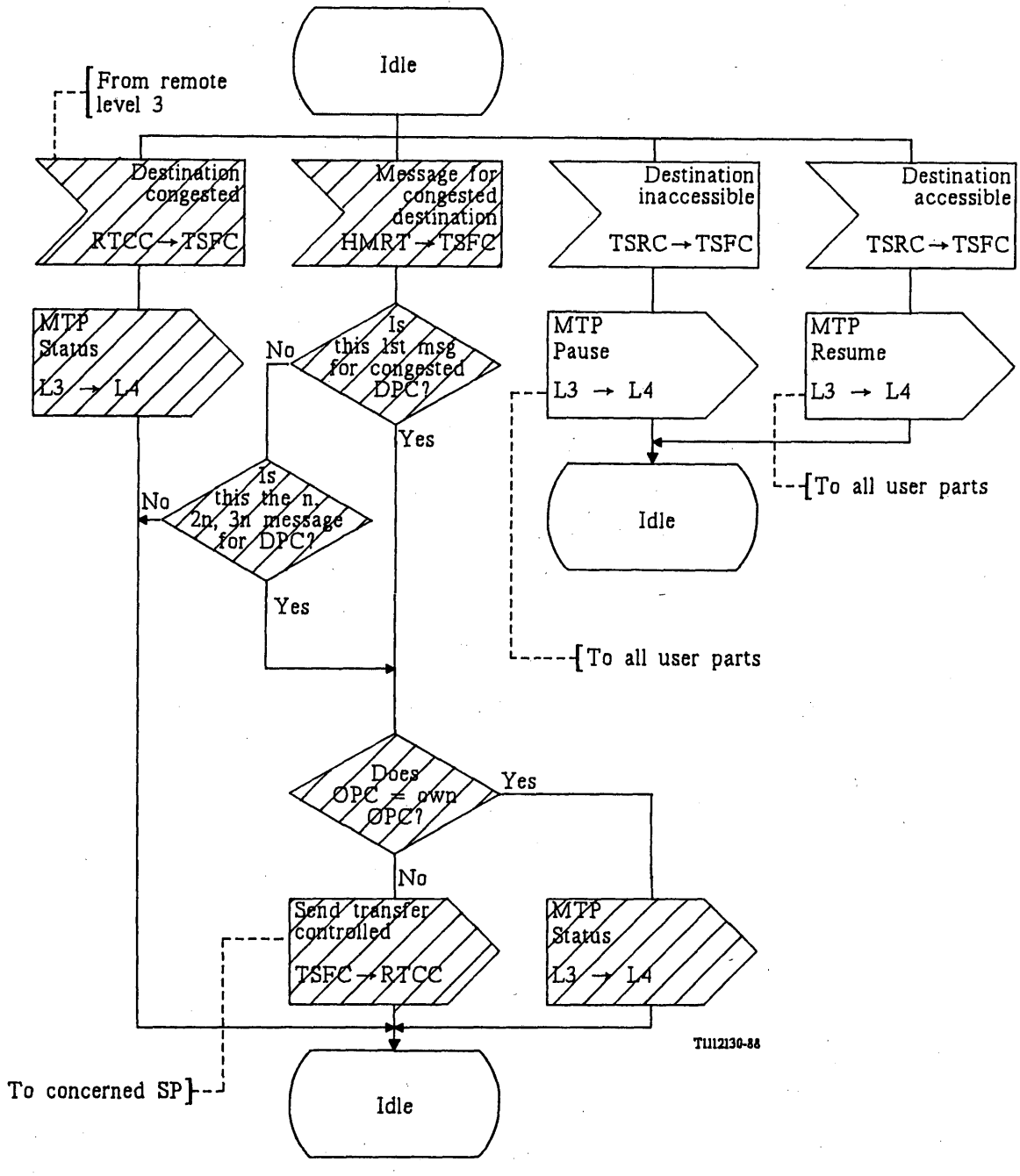
**Signalling traffic management; forced rerouting control (TFRC)**




*Note* – Dashed symbols apply only to the transfer restricted option.

FIGURE 33/Q.704

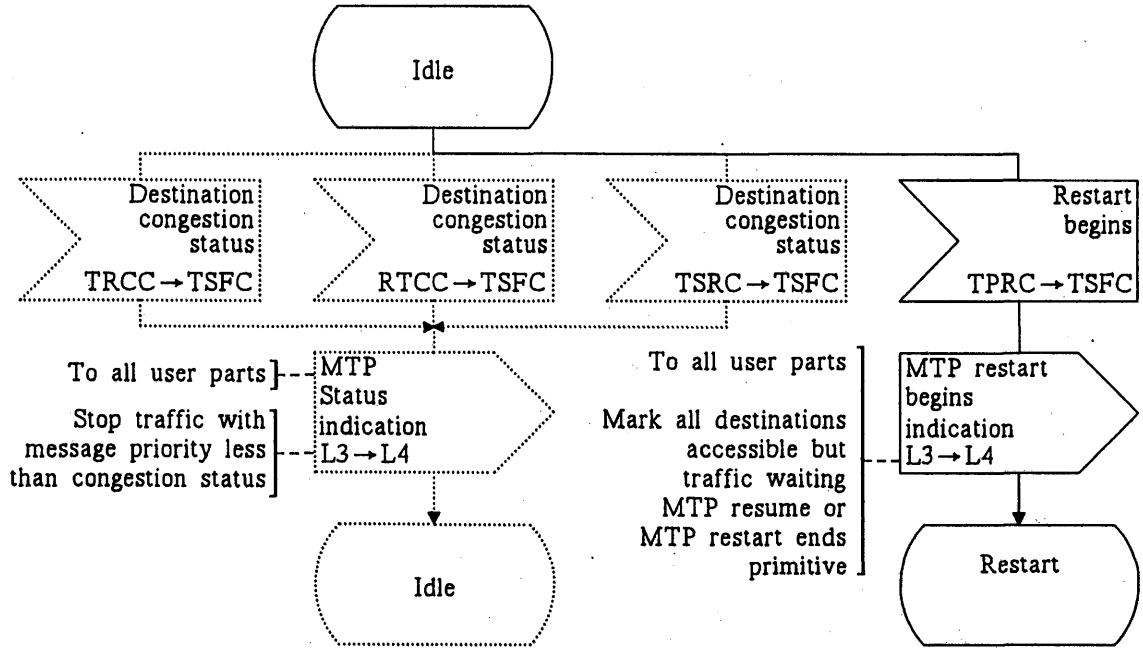
**Signalling traffic management; controlled rerouting control (TCRC)**




*Note* – Delete hatched symbols when using Multiple Congestion States option.

FIGURE 34a/Q704 (Sheet 1 of 3)

**Signalling traffic management; signalling traffic flow control (TSFC)**




*Note* – Dotted symbols apply only to the Multiple Congestion States option.

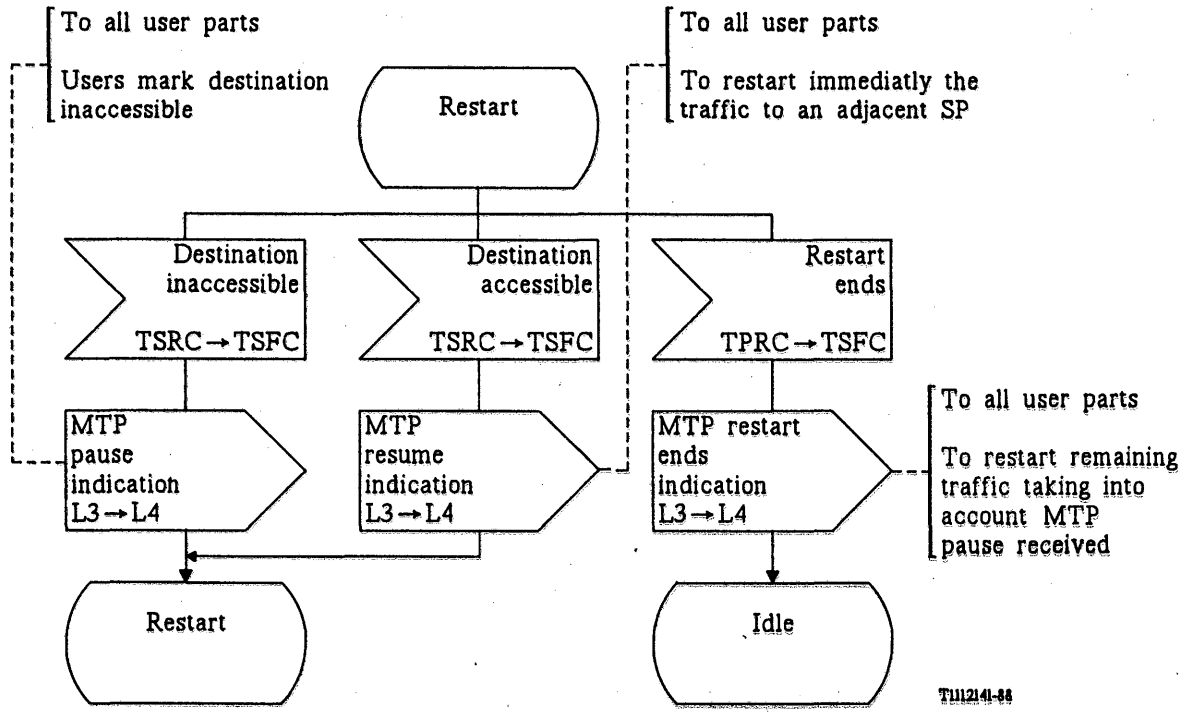



FIGURE 34a/Q.704 (Sheet 2 of 3)

**Signalling traffic management; signalling traffic flow control (TSFC)**

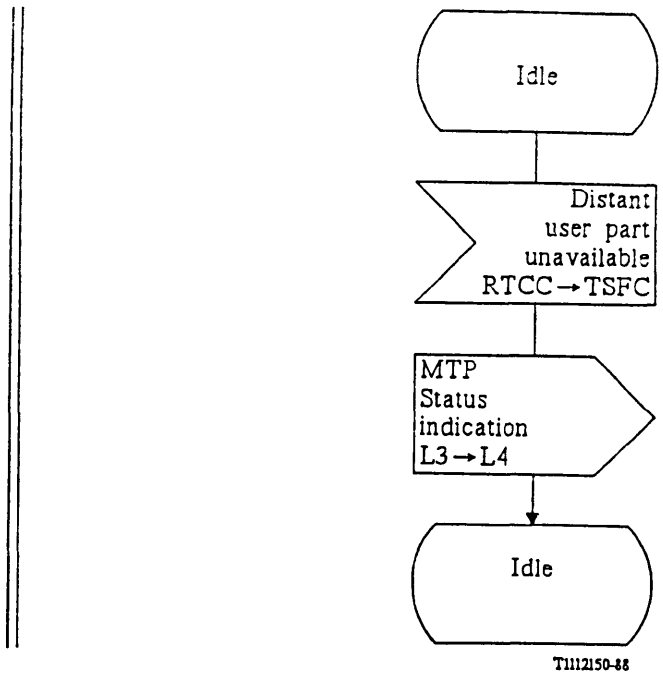



FIGURE 34a/Q704 (Sheet 3 of 3)

**Signalling traffic management; signalling traffic flow control (TSFC)**

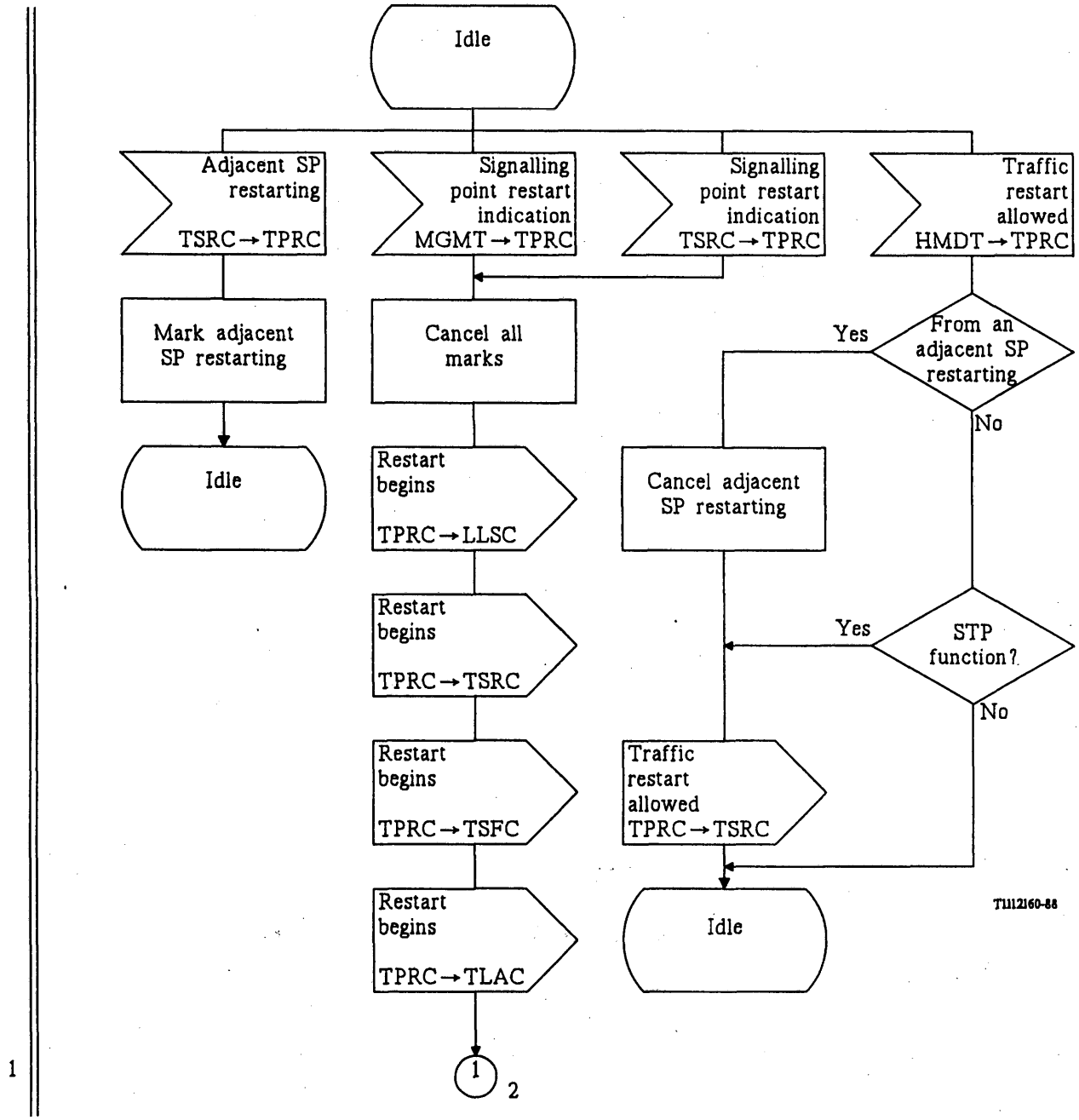



FIGURE 34b/Q.704 (Sheet 1 of 6)

**Signalling traffic management; signalling point restart control (TPRC)**

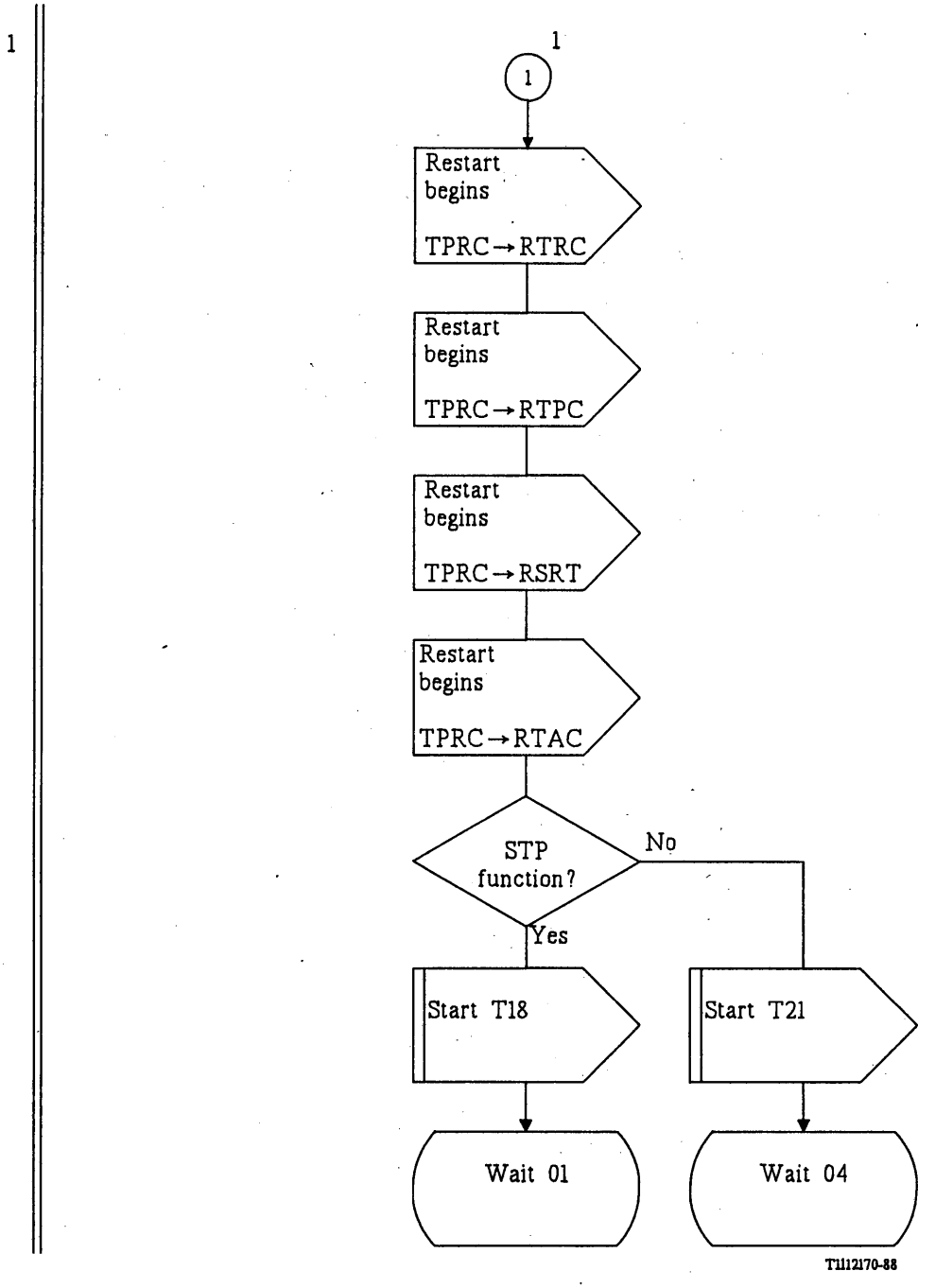



FIGURE 34b/Q.704 (Sheet 2 of 6)

**Signalling traffic management; signalling point restart control (TPRC)**

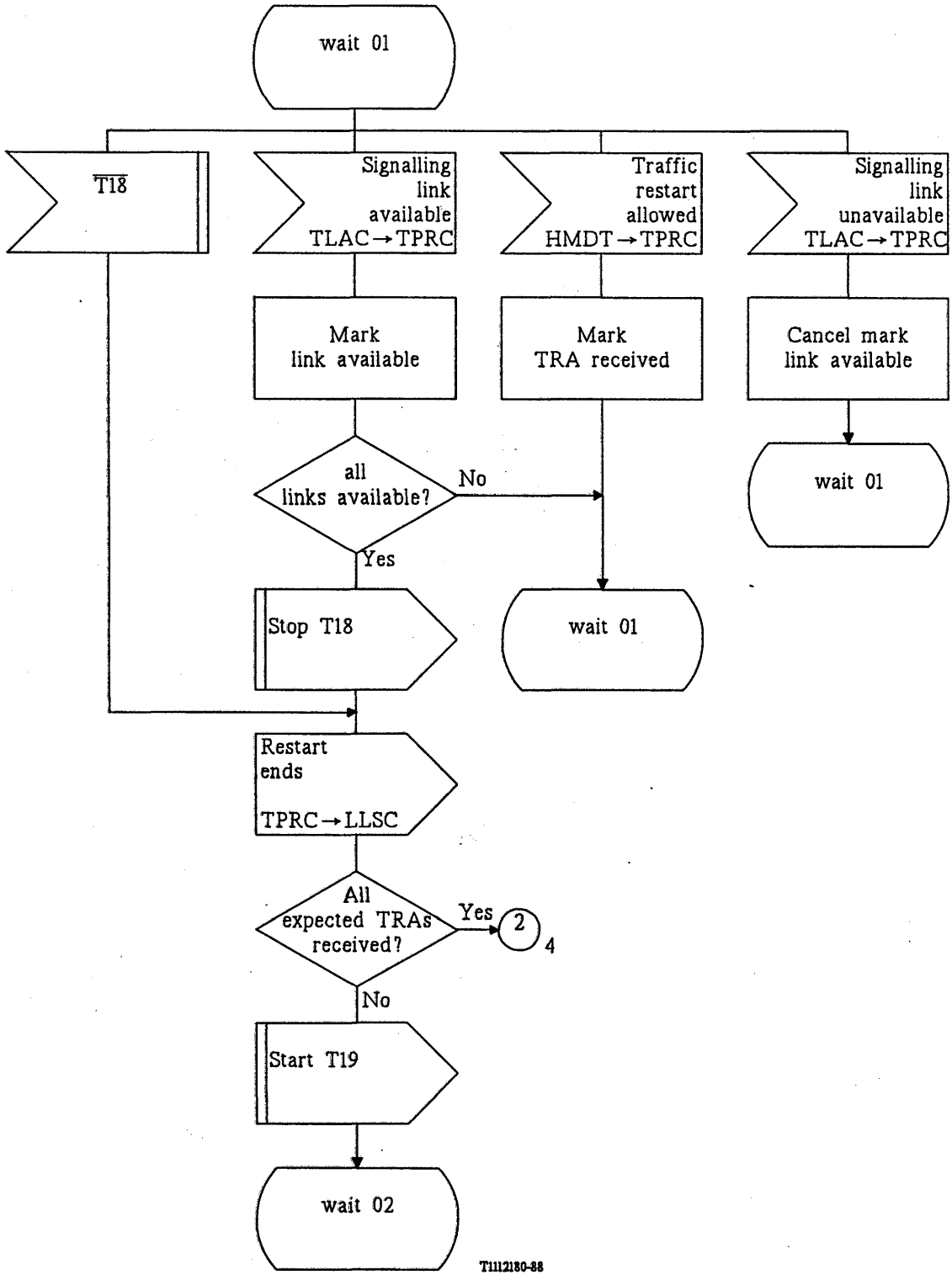



FIGURE 34b/Q.704 (Sheet 3 of 6)

**Signalling traffic management; signalling point restart control (TPRC)**

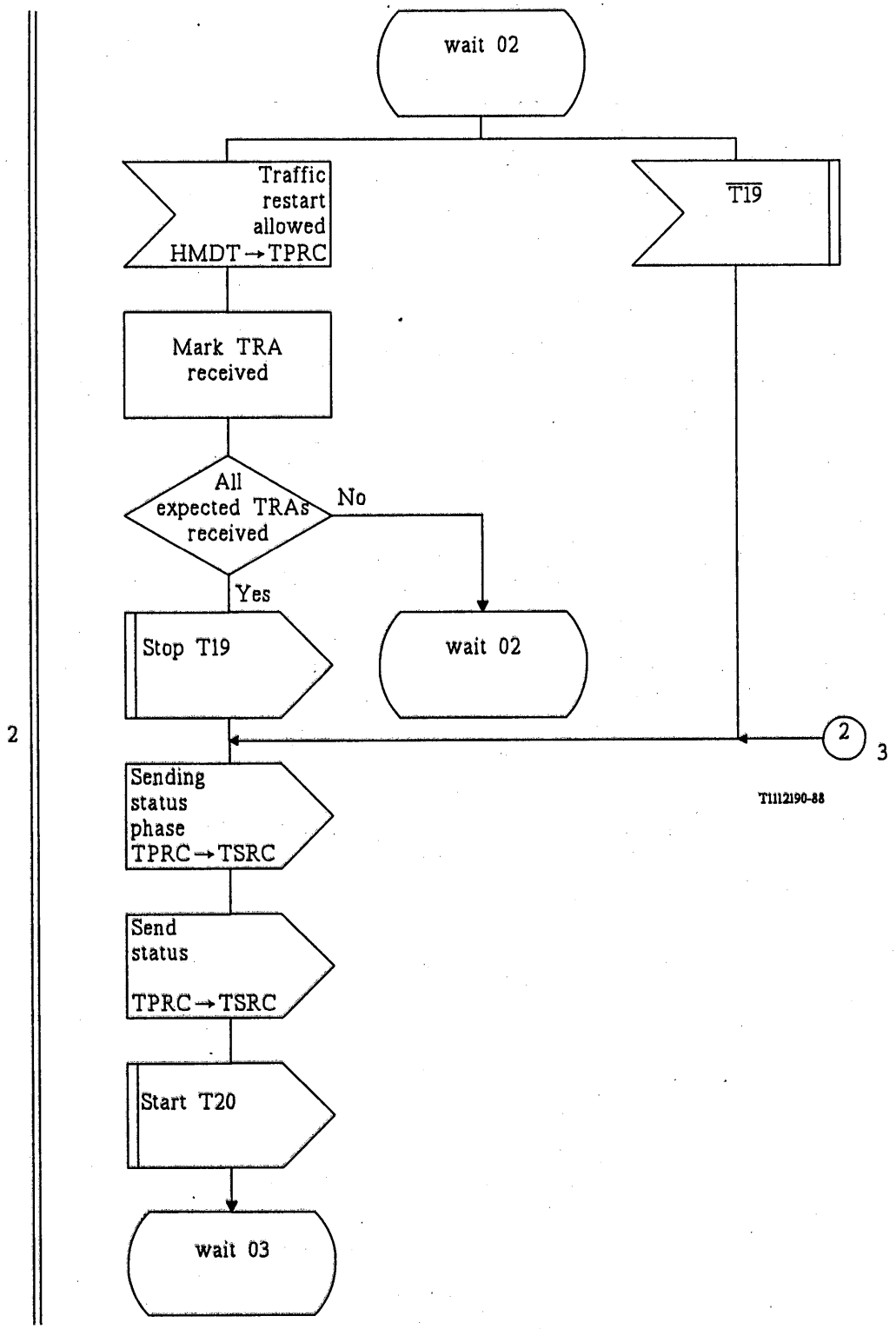



FIGURE 34b/Q.704 (Sheet 4 of 6)

**Signalling traffic management; signalling point restart control (TPRC)**

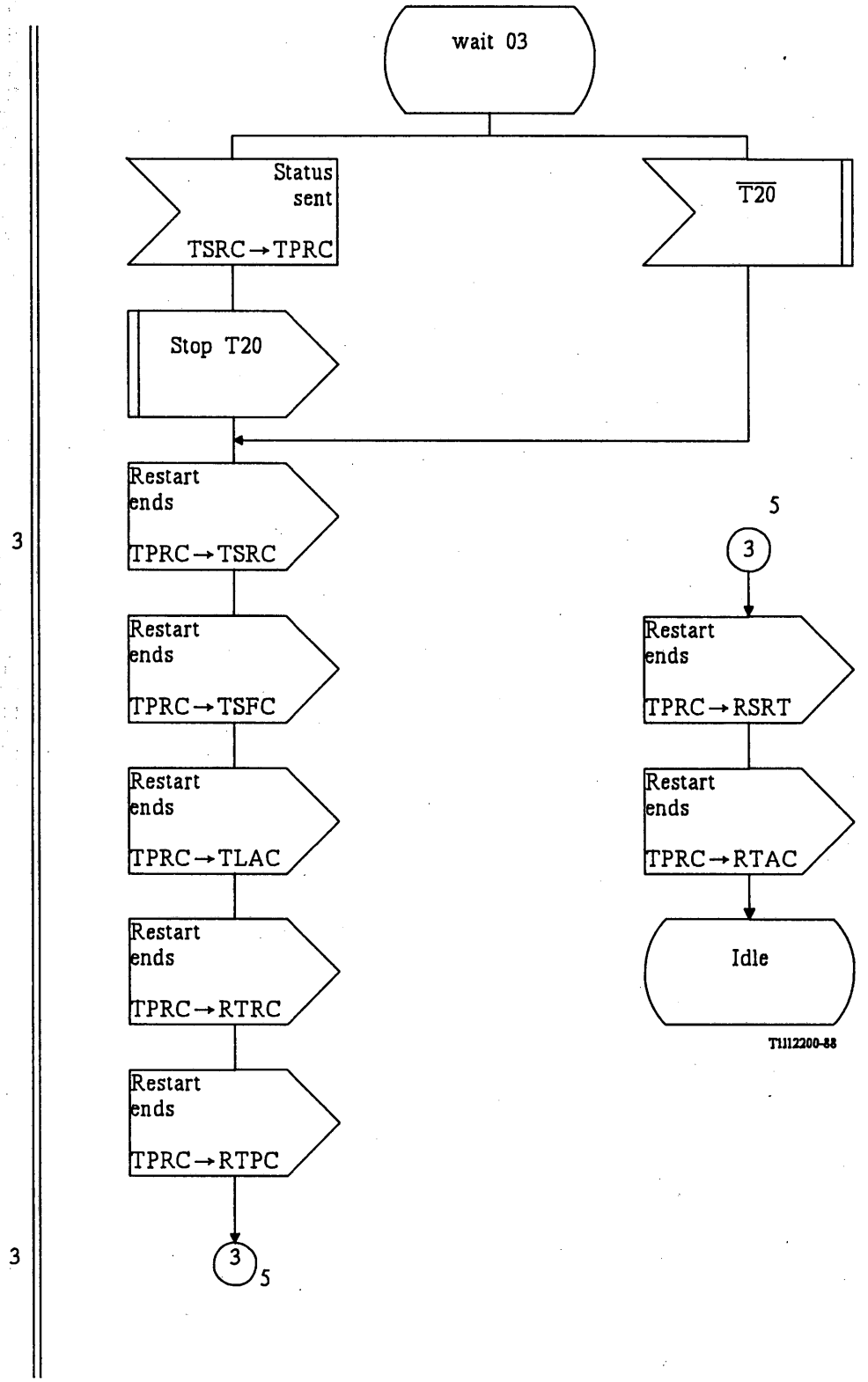



FIGURE 34b/Q.704 (Sheet 5 of 6)

**Signalling traffic management; signalling point restart control (TPRC)**

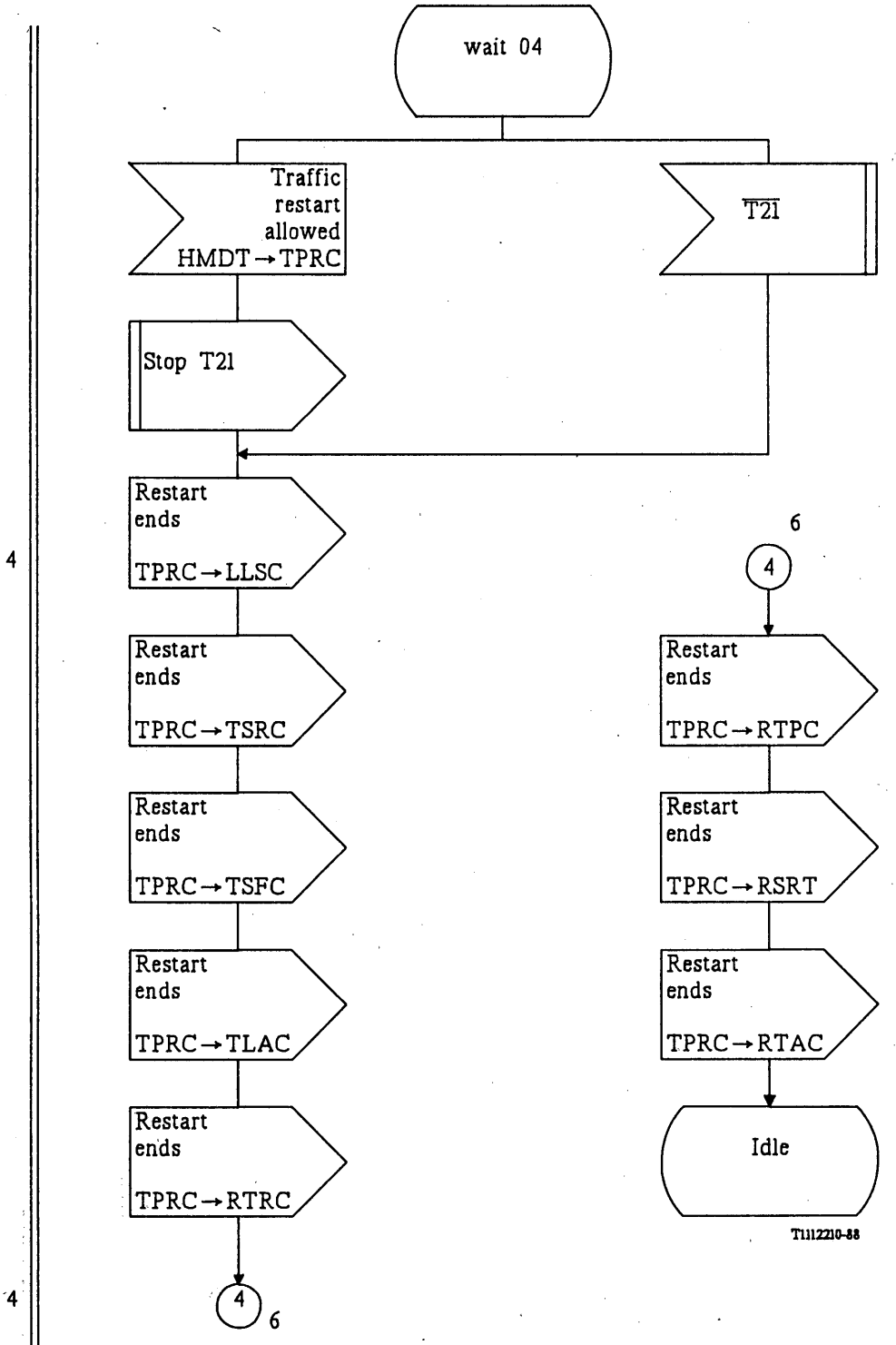
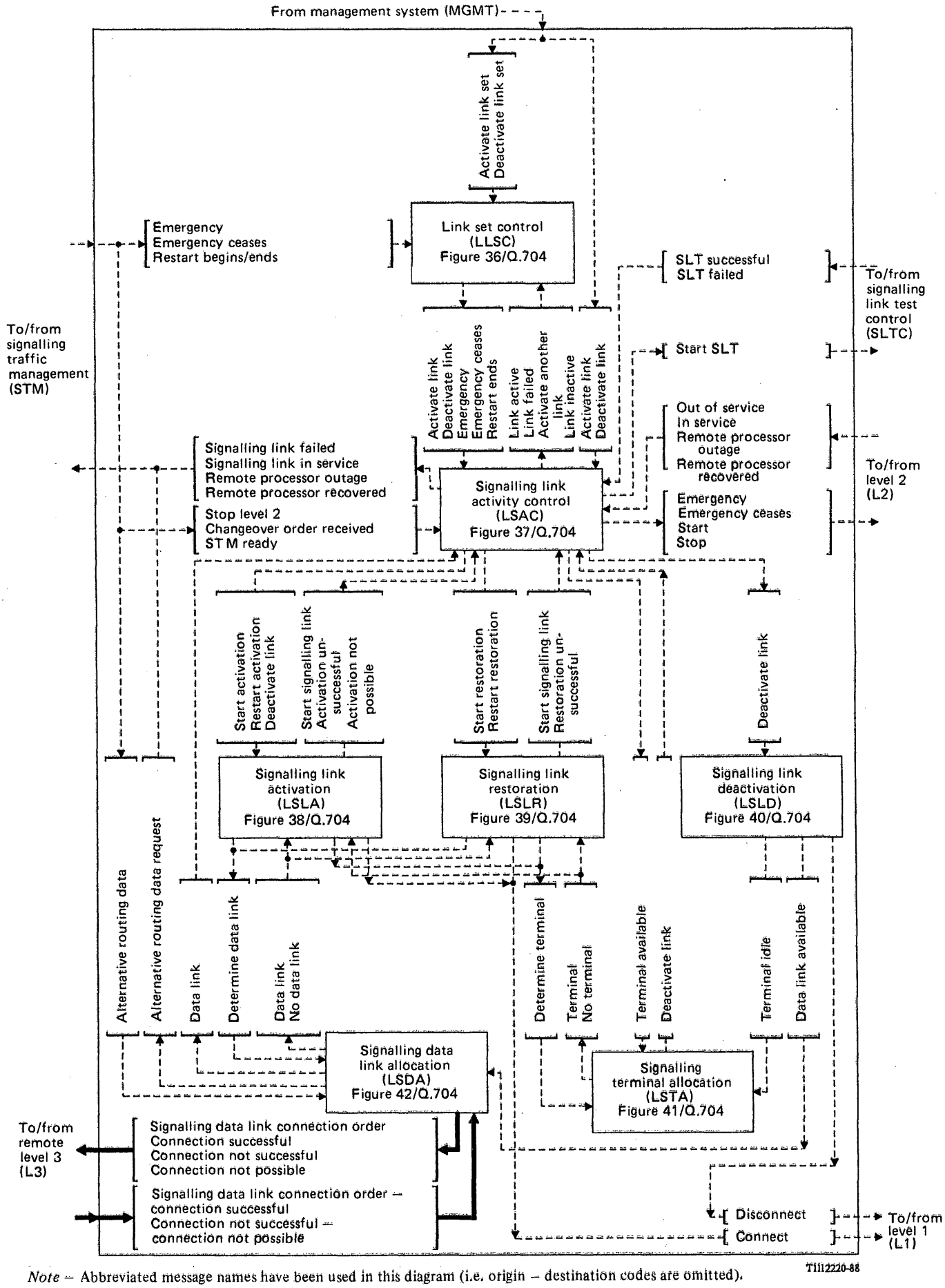



FIGURE 34b/Q.704 (Sheet 6 of 6)

**Signalling traffic management; signalling point restart control (TPRC)**




*Note* – Abbreviated message names have been used in this diagram (i.e. origin – destination codes are omitted).

FIGURE 35/Q.704

**Level 3 – Signalling link management (SLM); functional block interactions**

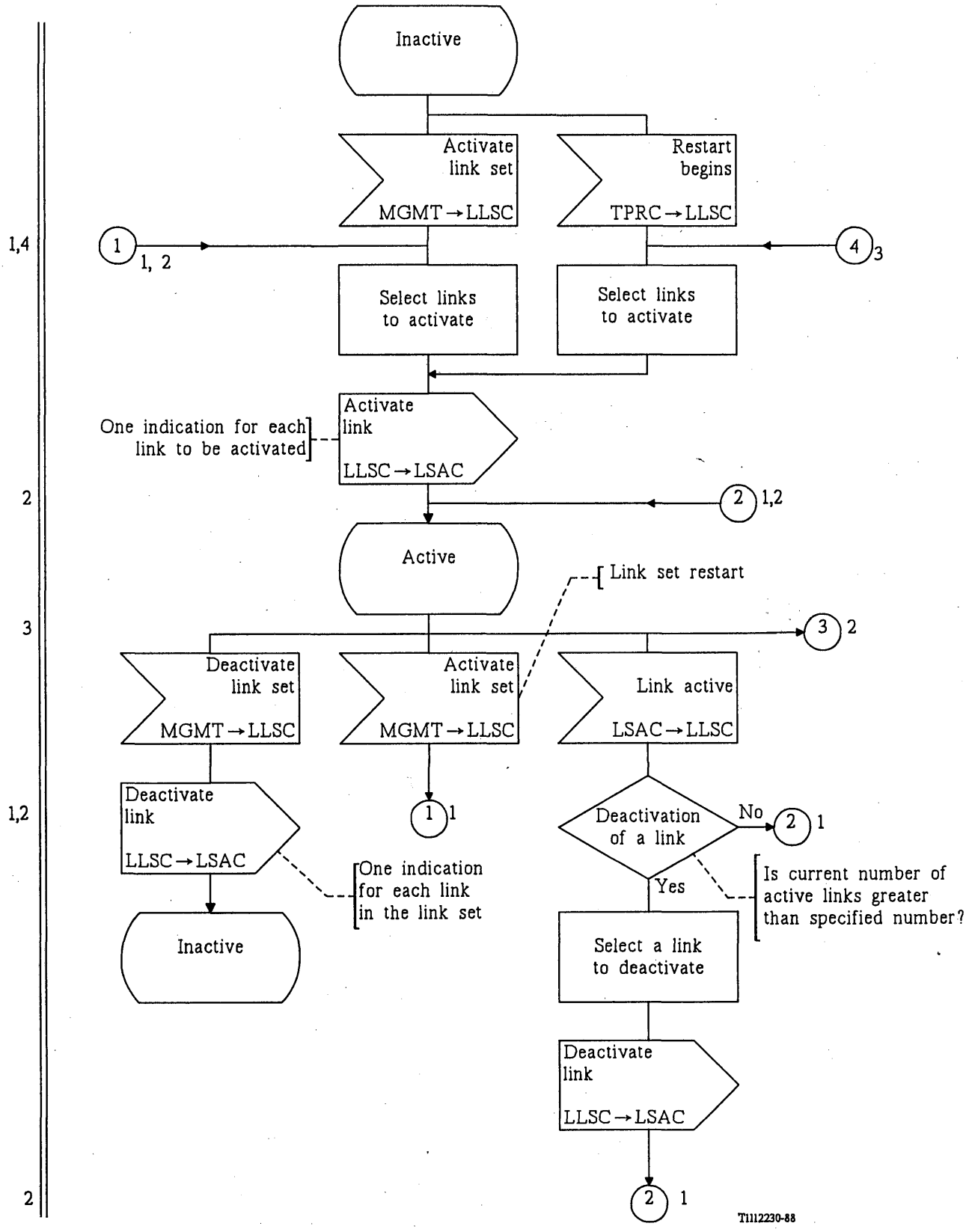
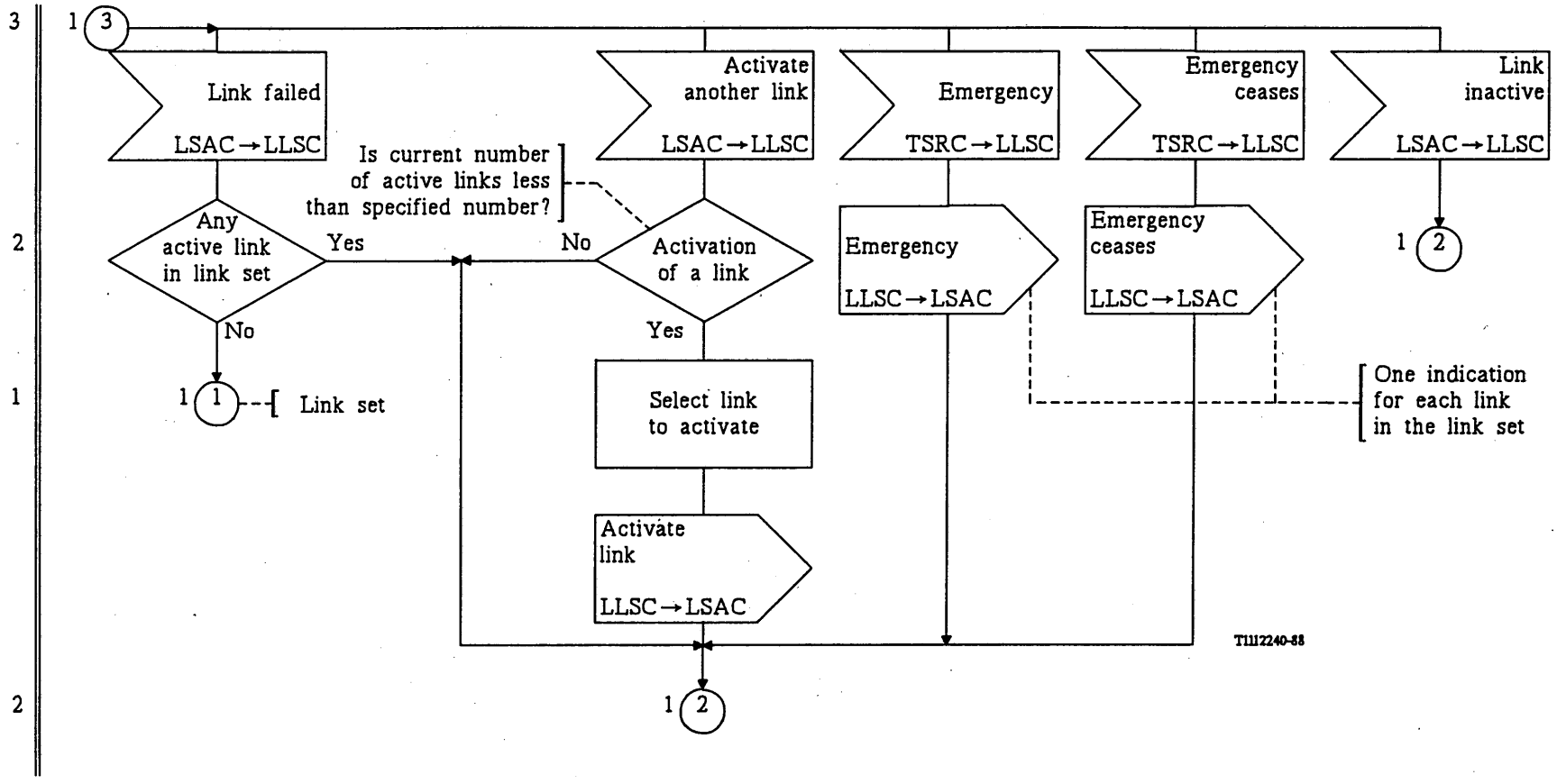



FIGURE 36/Q.704 (sheet 1 of 3)

**Signalling link management; link set control (LLSC)**




*Note 1* – It is assumed that this function has access to information regarding the number and status of links in a link set.

*Note 2* – It should be ensured that signalling link activation and deactivation attempts are not made simultaneously for the same signalling link.

FIGURE 36/Q.704 (sheet 2 of 3)

**Signalling link management; link set control (LLSC)**

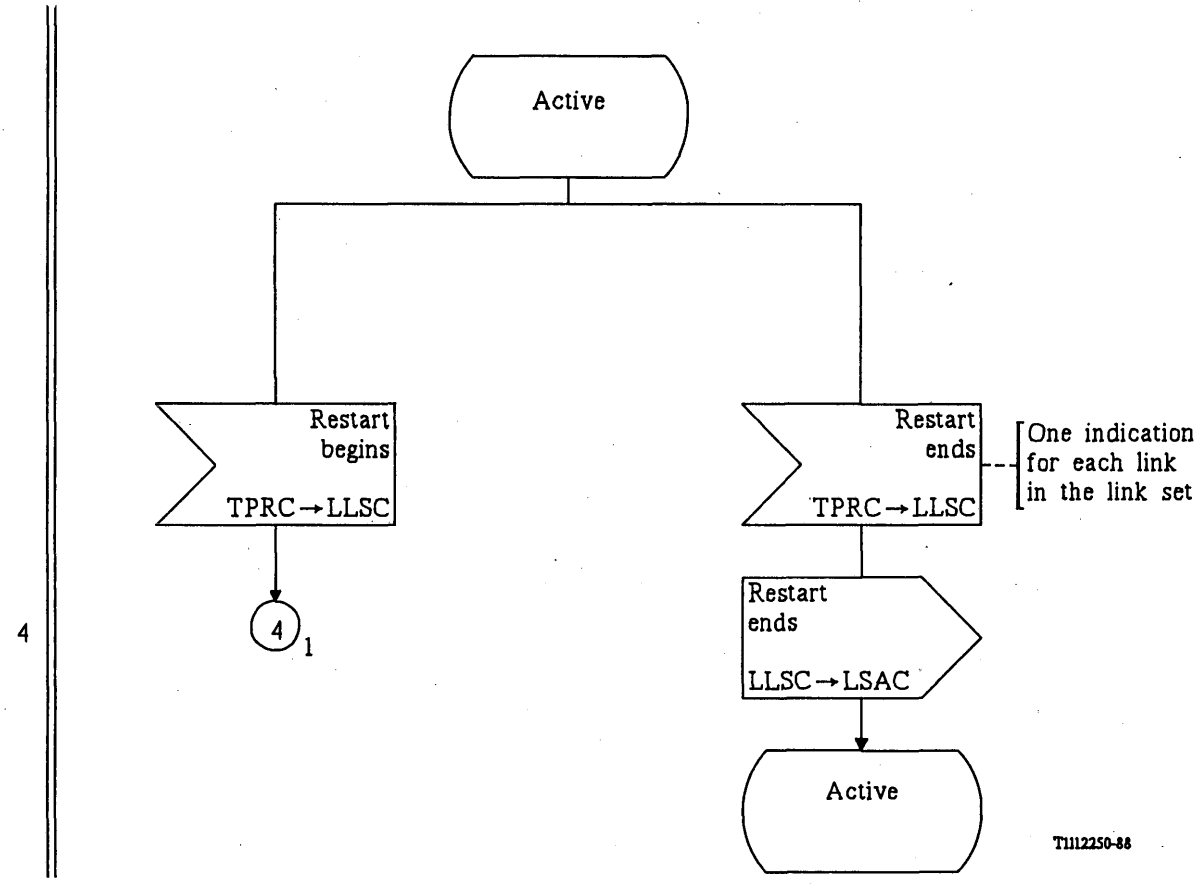



FIGURE 36/Q.704 (sheet 3 of 3)

**Signalling link management; link set control (LLSC)**

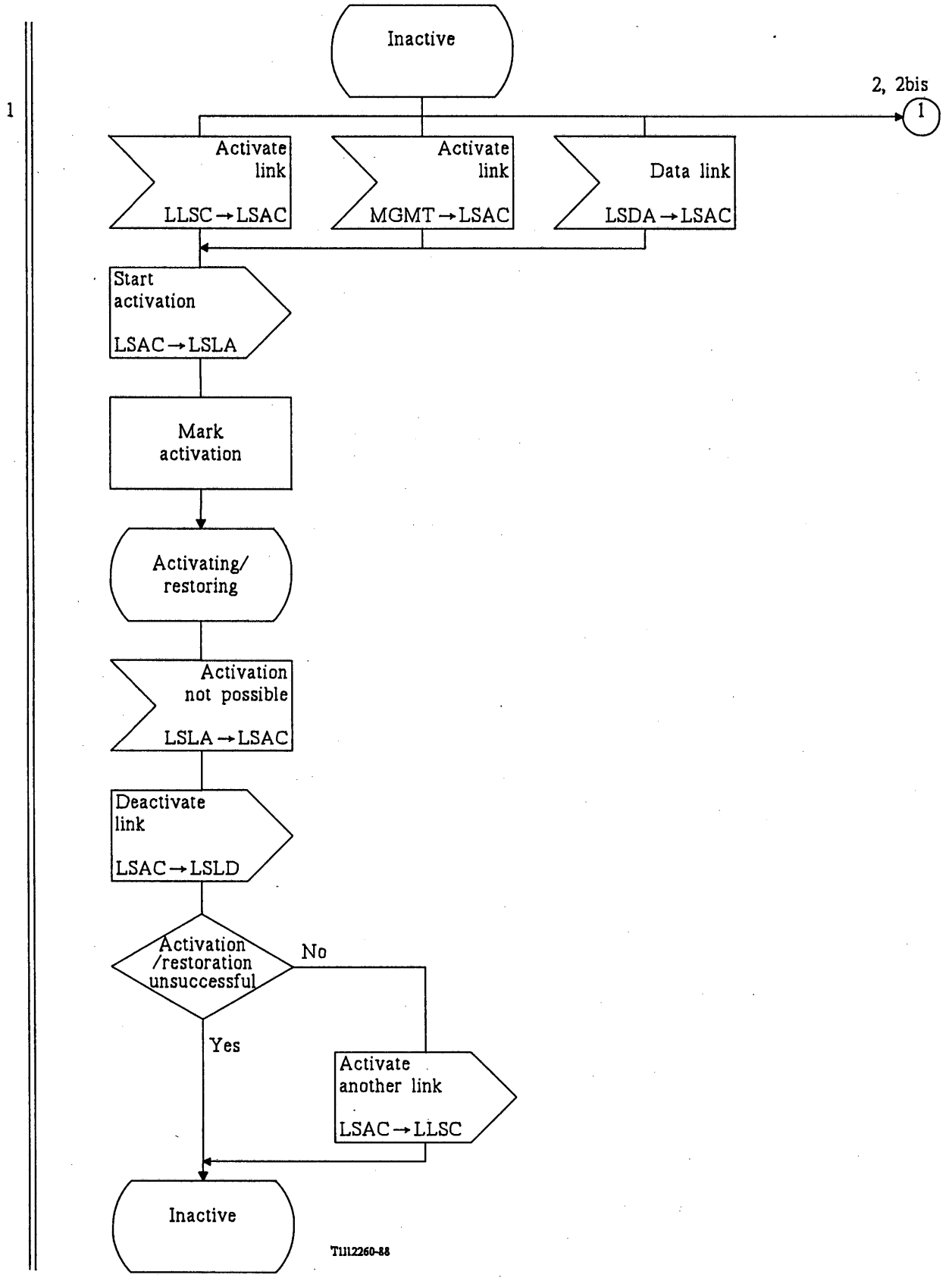
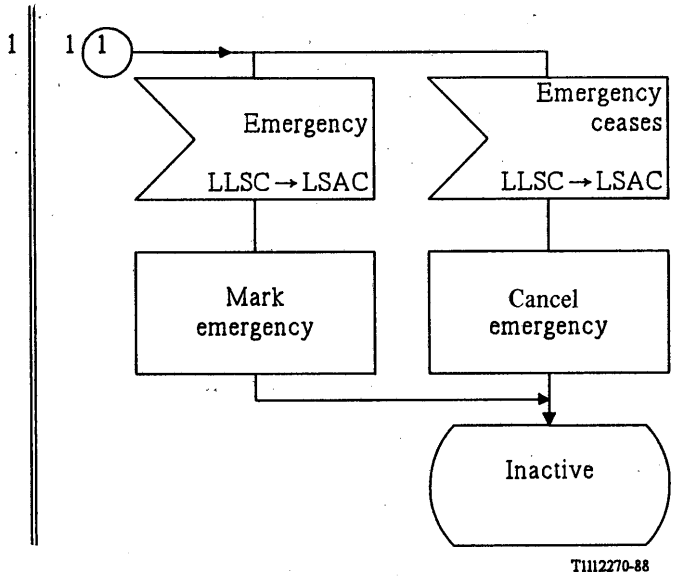



FIGURE 37/Q.704 (sheet 1 of 10)

Signalling link management; signalling link activity control (LSAC)




*Note* – See sheet 2*bis*, for a national option.

FIGURE 37/Q.704 (sheet 2 of 10)

**Signalling link management; signalling link activity control (LSAC)**

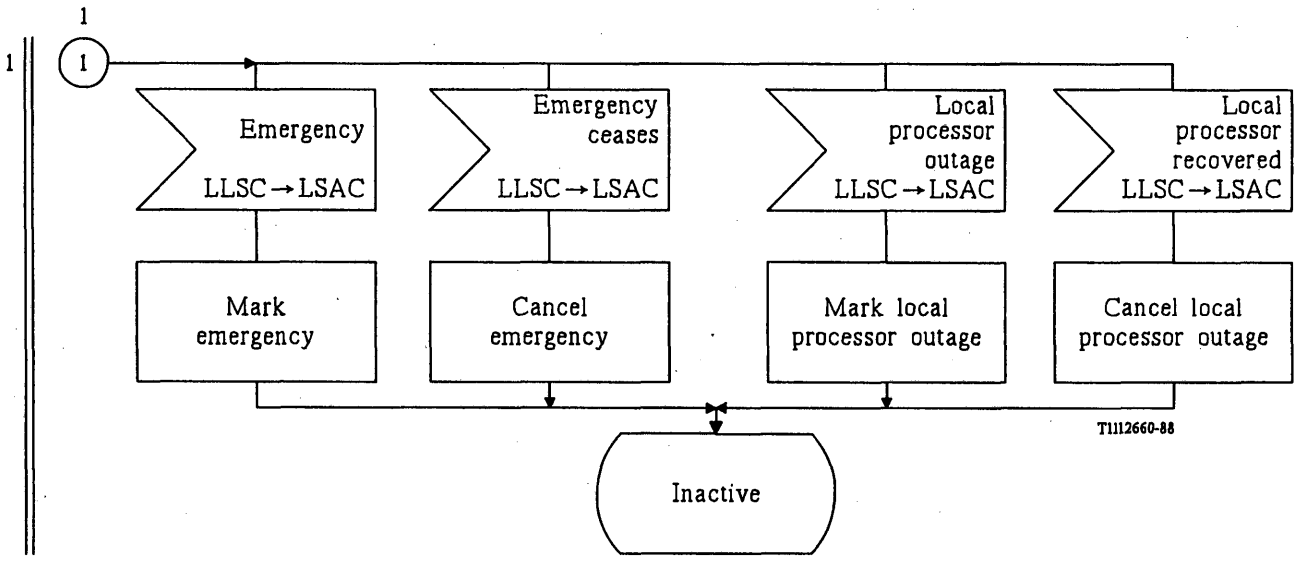



FIGURE 37/Q.704 (sheet 2*bis* of 10)

**Signalling link management; signalling link activity control (LSAC)**

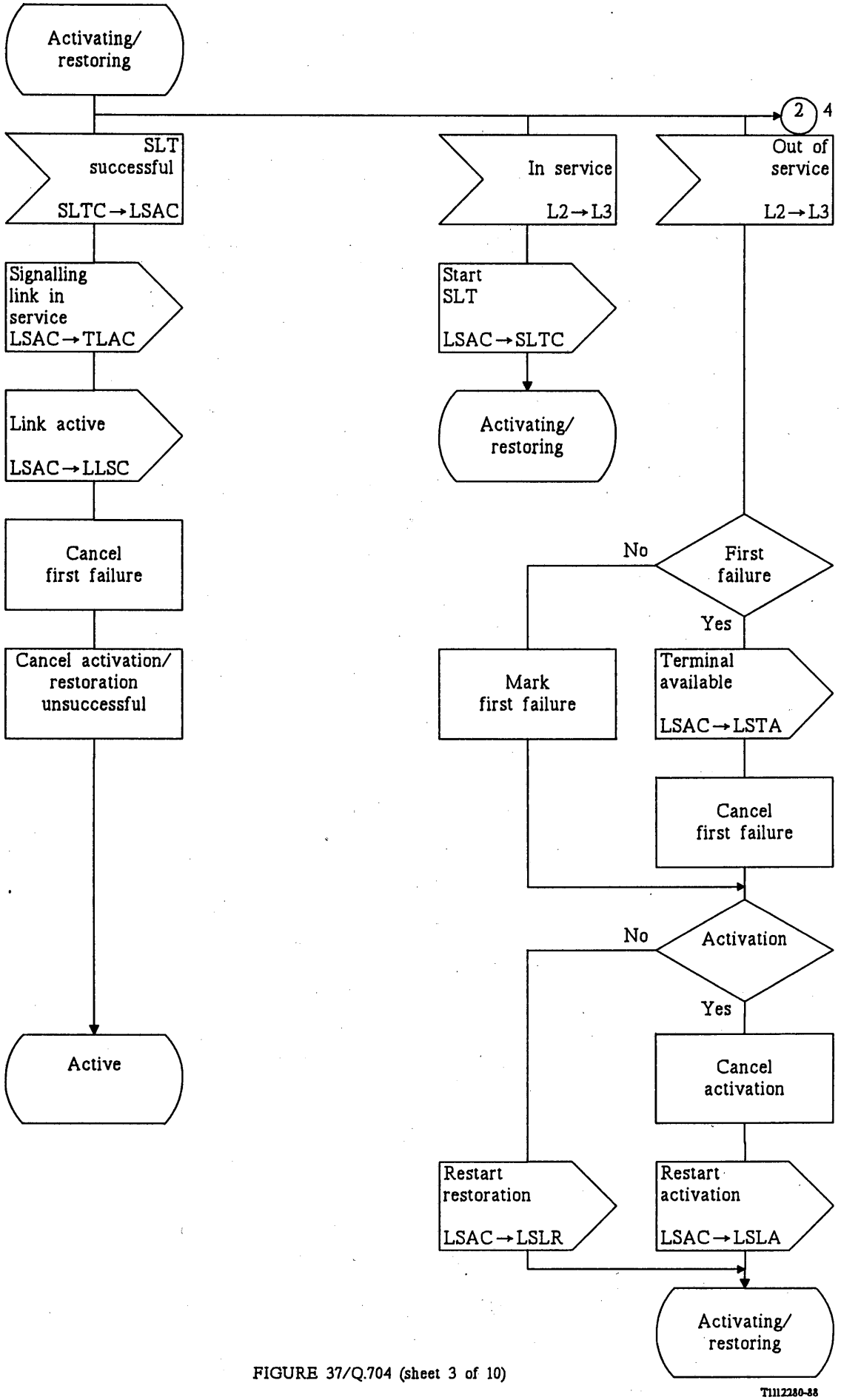



FIGURE 37/Q.704 (sheet 3 of 10)

**Signalling link management; signalling link activity control (LSAC)**

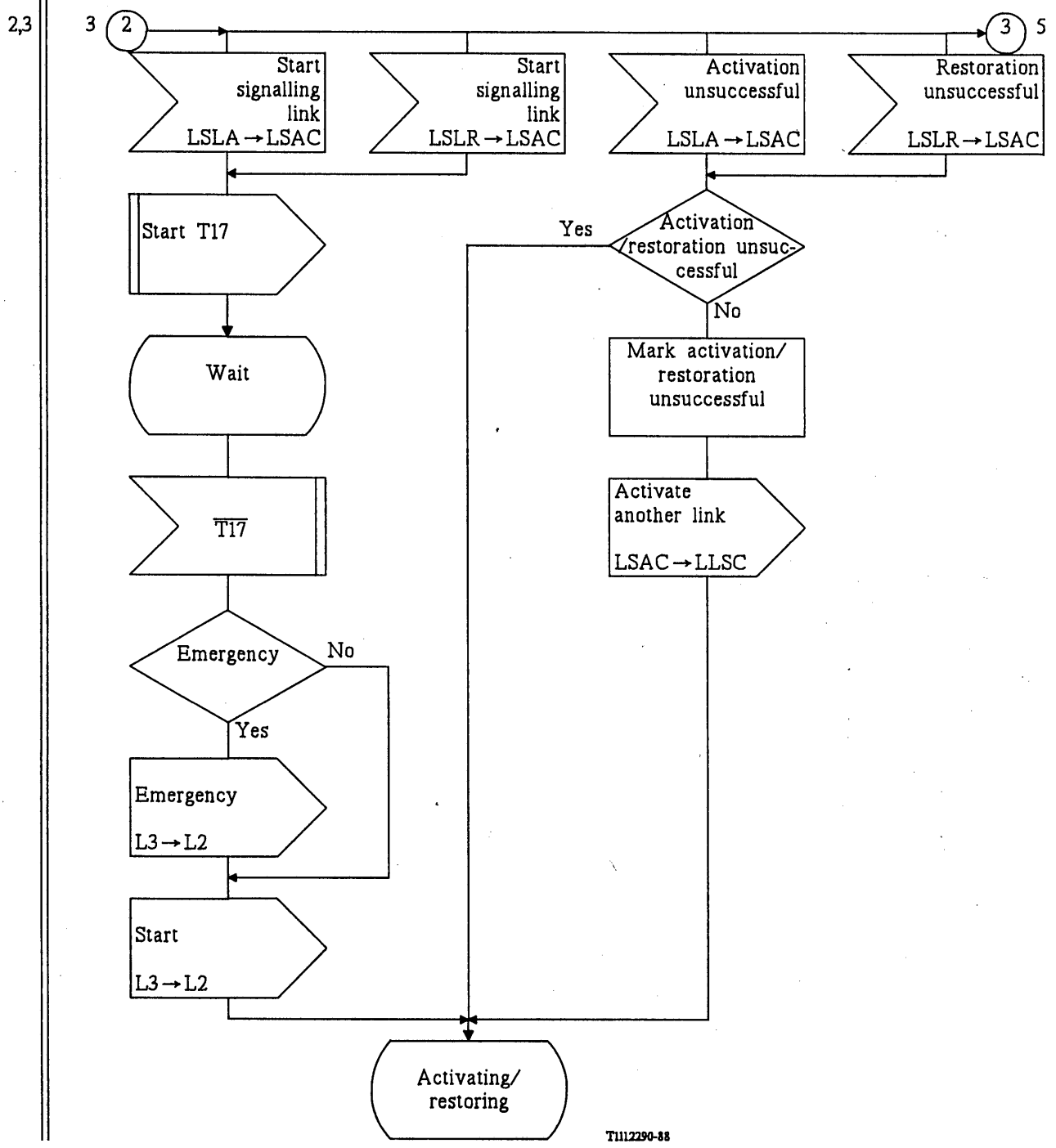



FIGURE 37/Q.704 (sheet 4 of 10)

Signalling link management; signalling link activity control (LSAC)

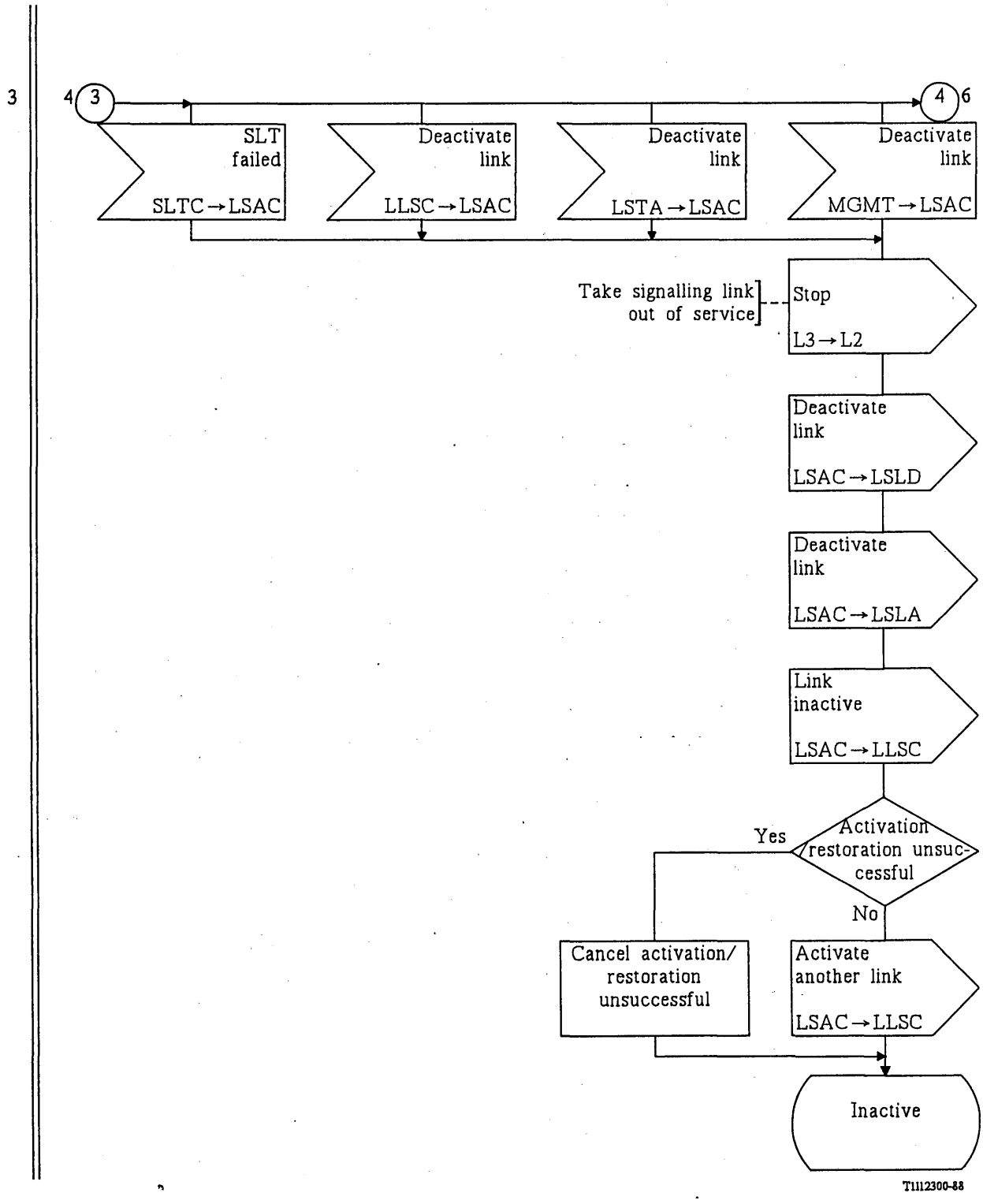



FIGURE 37/Q.704 (sheet 5 of 10)

**Signalling link management; signalling link activity control (LSAC)**

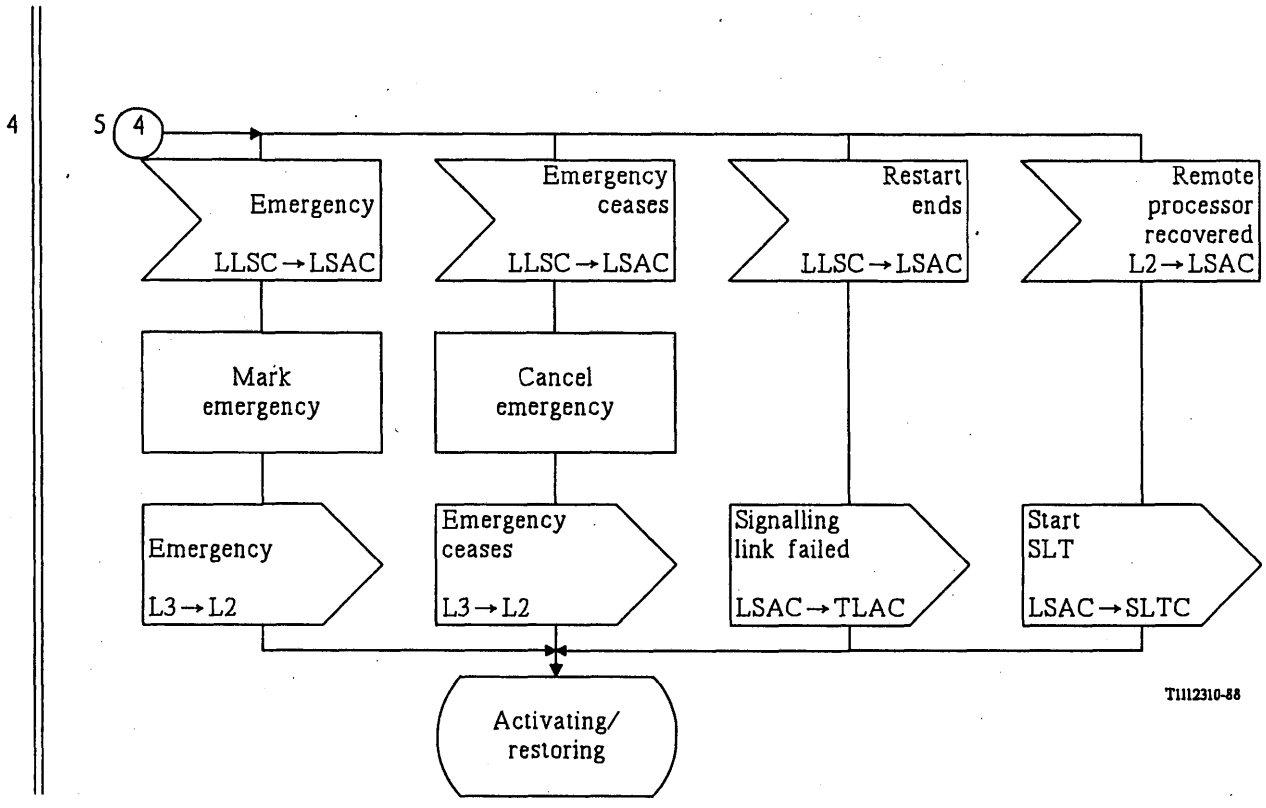



FIGURE 37/Q.704 (sheet 6 of 10)

**Signalling link management; signalling link activity control (LSAC)**

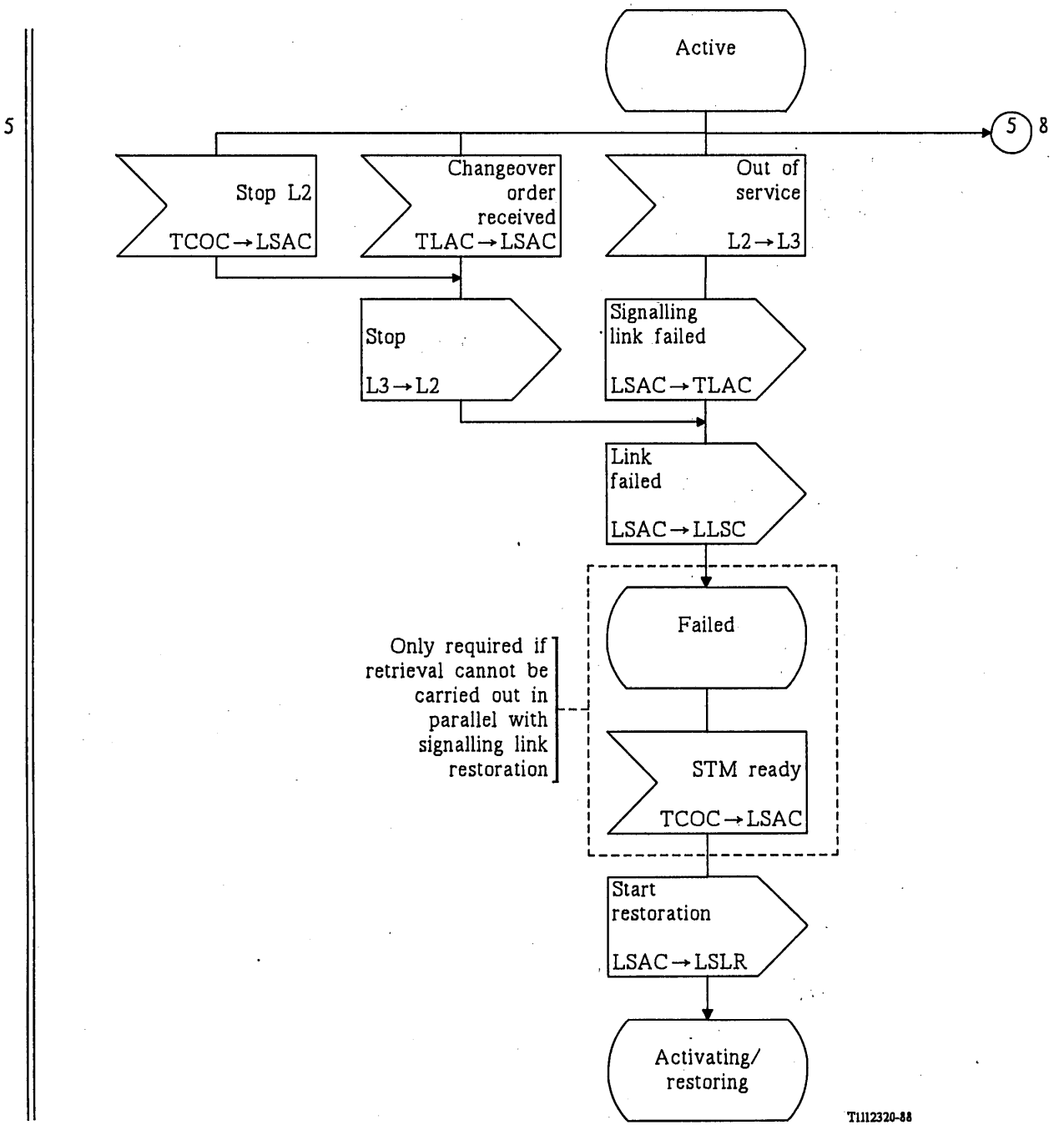



FIGURE 37/Q.704 (sheet 7 of 10)

**Signalling link management; signalling link activity control (LSAC)**

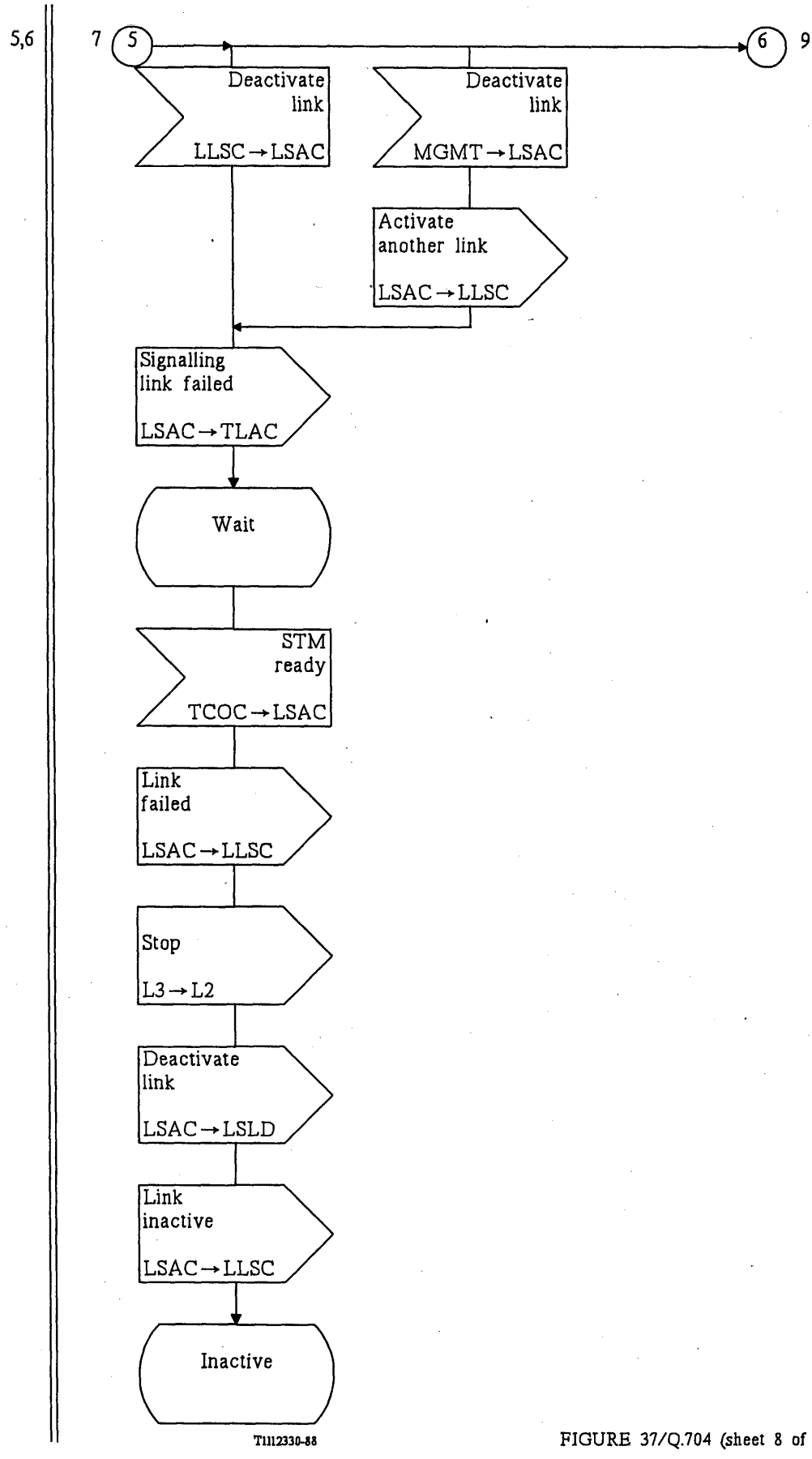



FIGURE 37/Q.704 (sheet 8 of 10)

**Signalling link management; signalling link activity control (LSAC)**

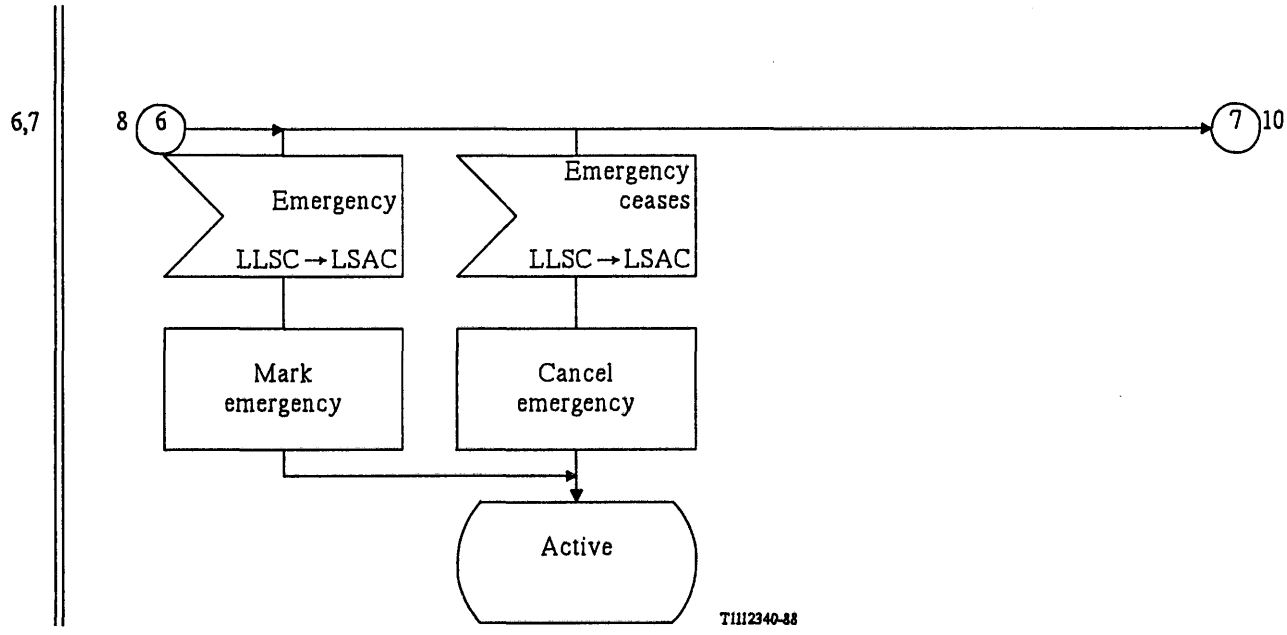
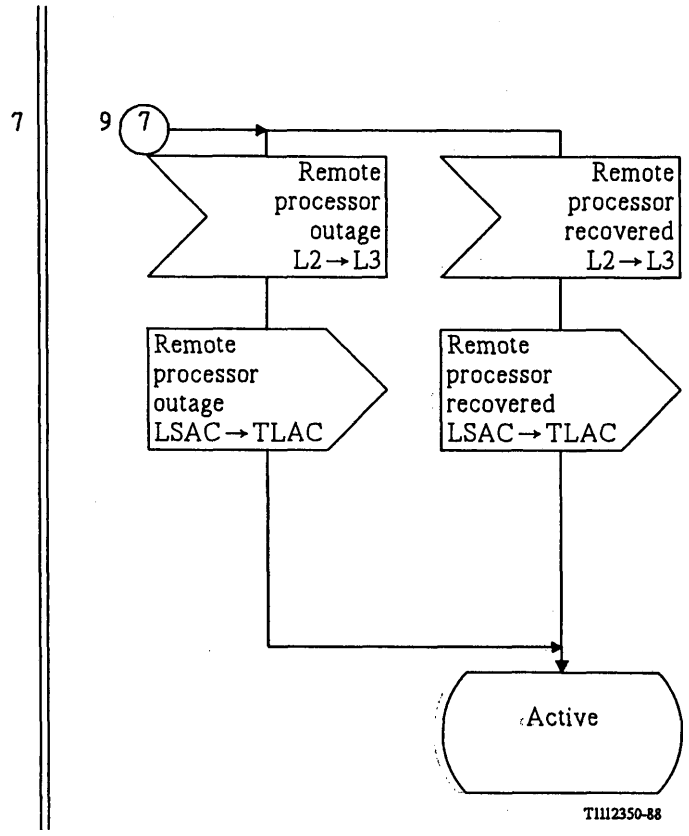



FIGURE 37/Q.704 (sheet 9 of 10)

**Signalling link management; signalling link activity control (LSAC)**




*Note* – See sheet 10*bis*, for a national option.

FIGURE 37/Q.704 (sheet 10 of 10)

**Signalling link management; signalling link activity control (LSAC)**

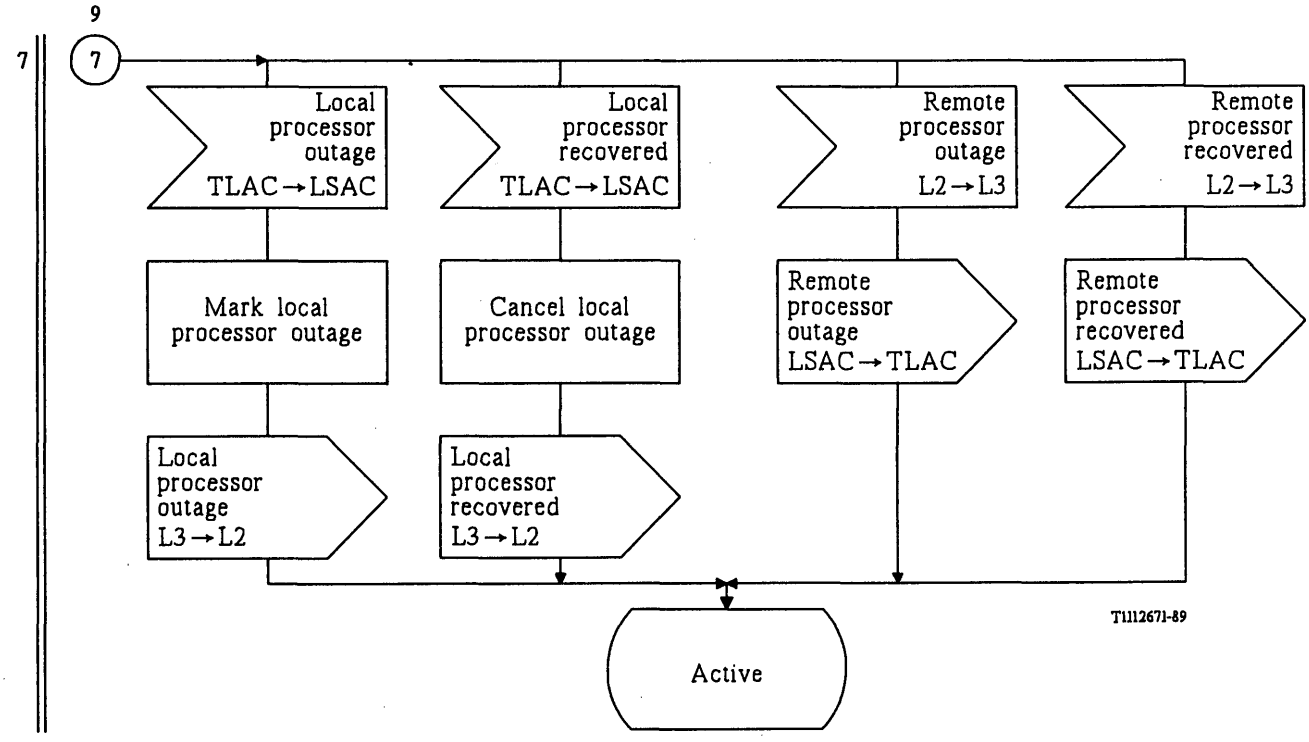



FIGURE 37/Q.704 (sheet 10*bis* of 10)

**Signalling link management; signalling link activity control (LSAC) (National option)**

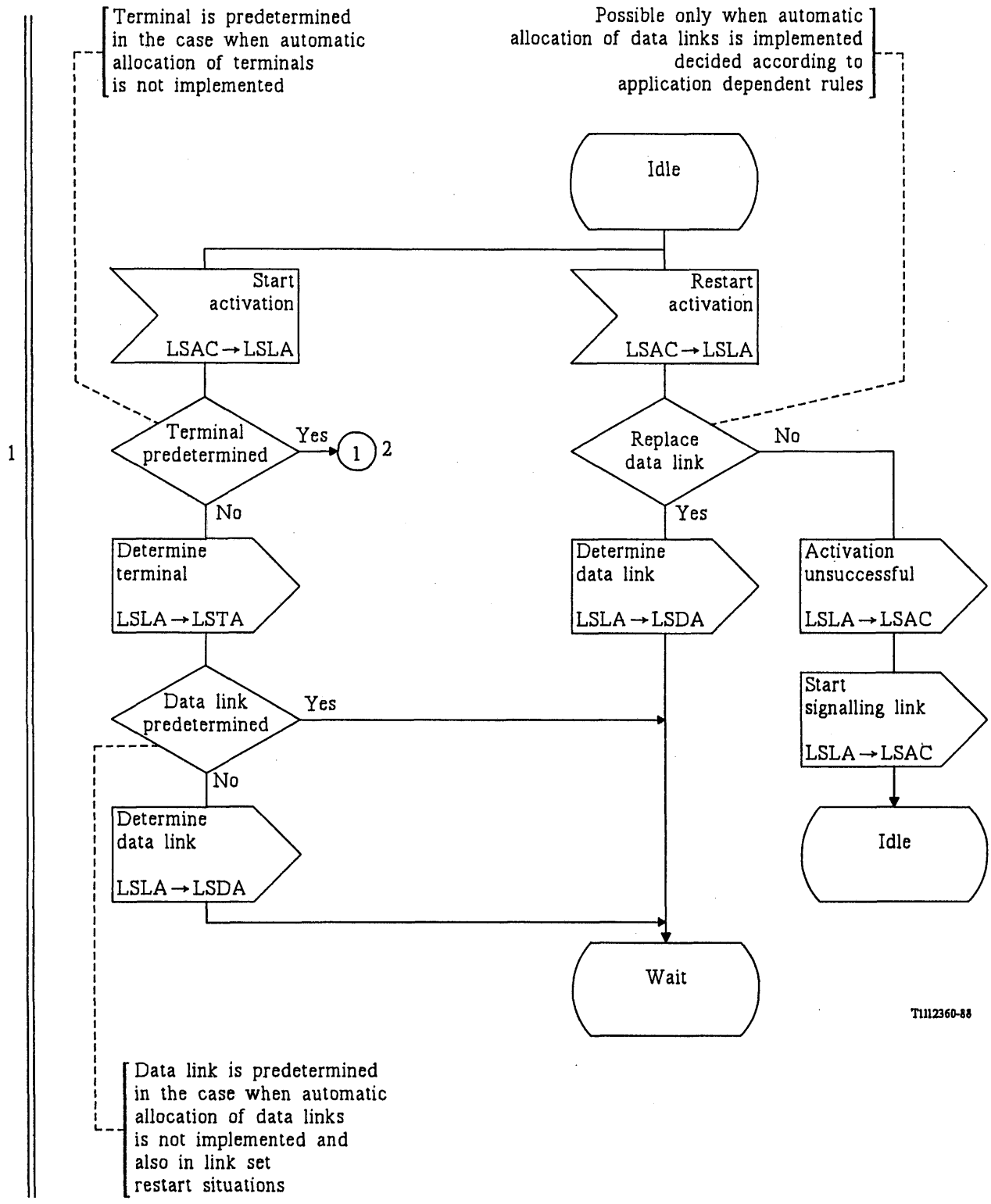



FIGURE 38/Q.704 (sheet 1 of 3)

**Signalling link management; signalling link activation (LSLA)**

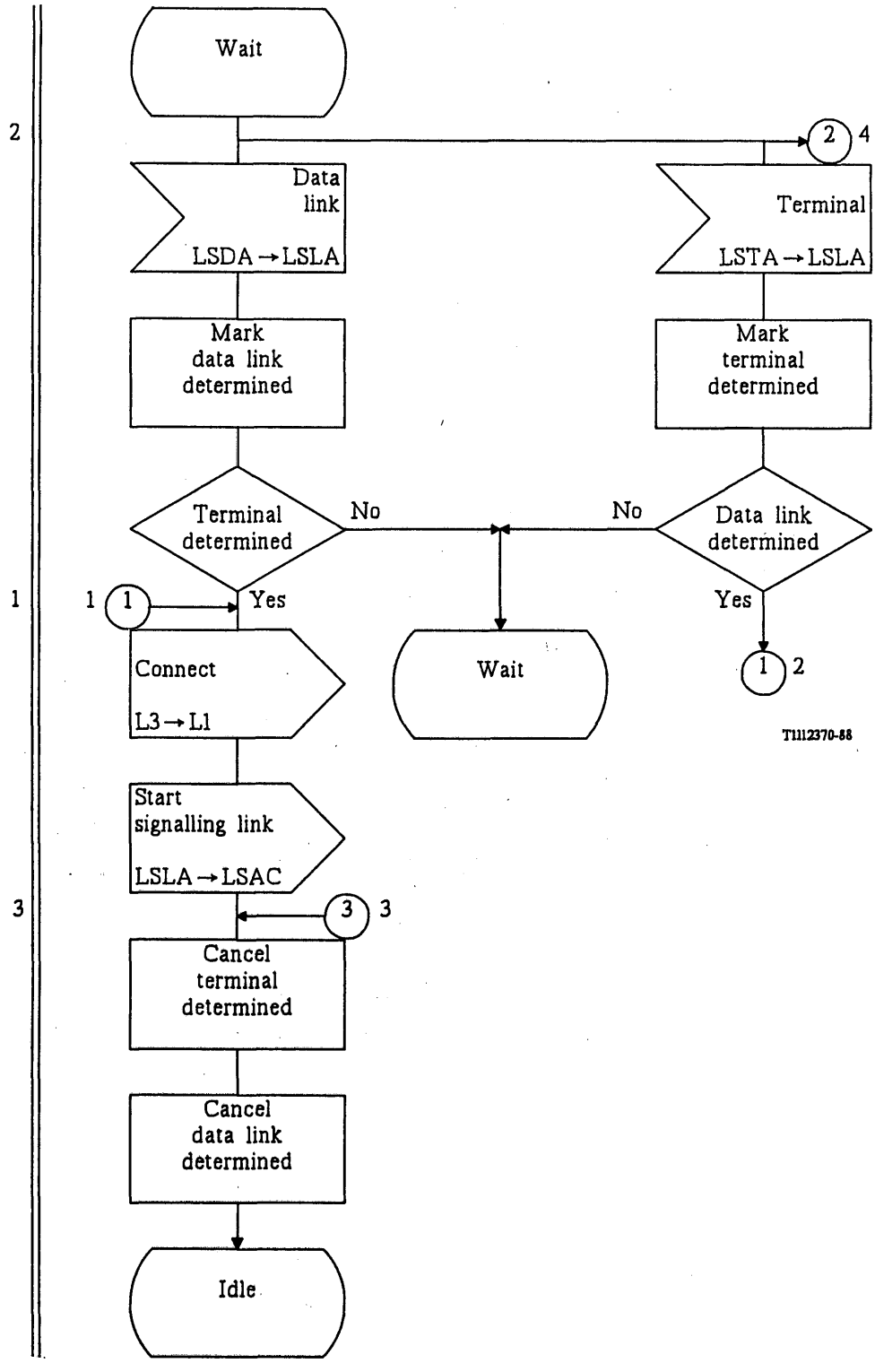



FIGURE 38/Q.704 (sheet 2 of 3)

**Signalling link management; signalling link activation (LSLA)**

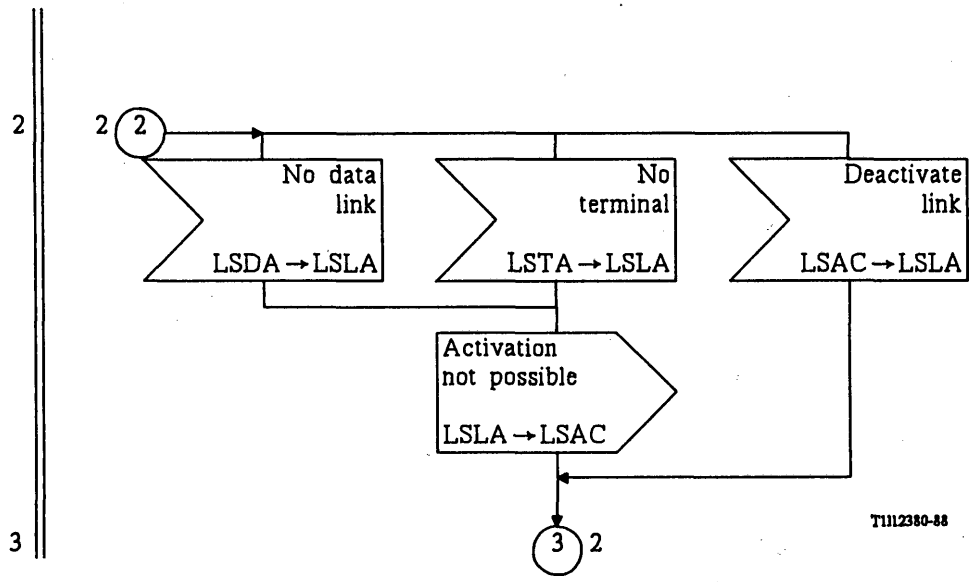



FIGURE 38/Q.704 (sheet 3 of 3)

**Signalling link management; signalling link activation (LSLA)**

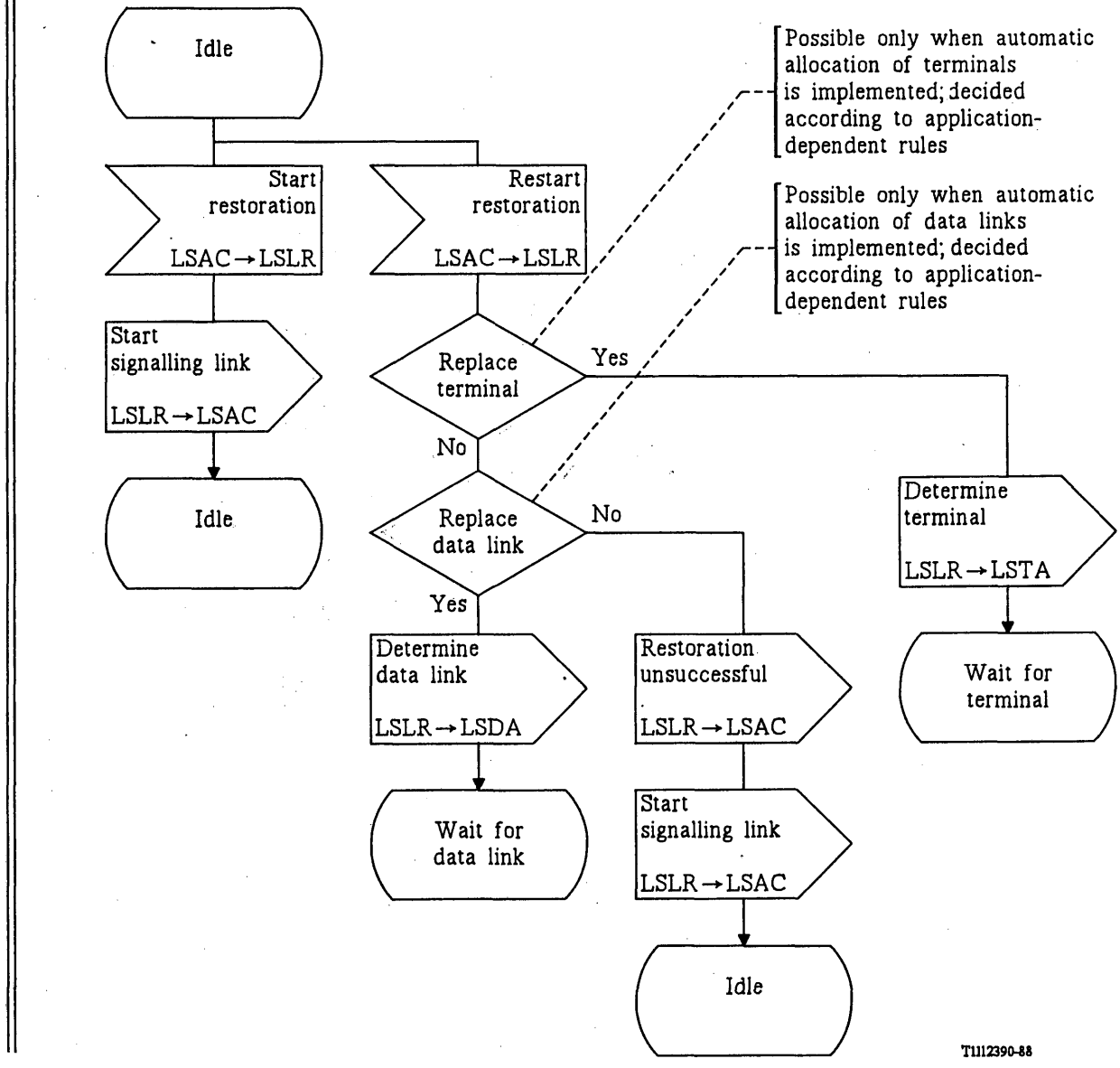



FIGURE 39/Q.704 (sheet 1 of 2)

**Signalling link management; signalling link restoration (LSLR)**

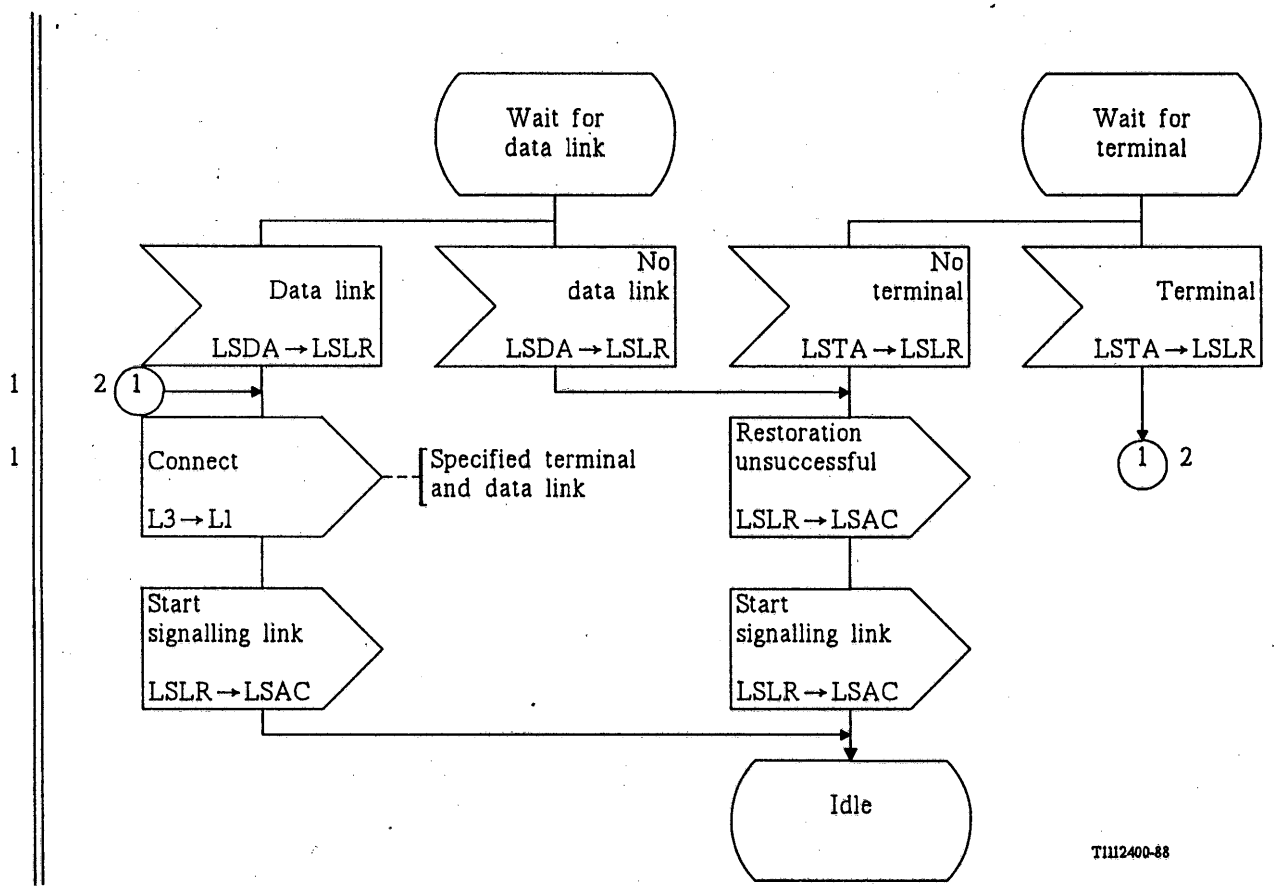



FIGURE 39/Q.704 (sheet 2 of 2)

**Signalling link management; signalling link restoration (LSLR)**

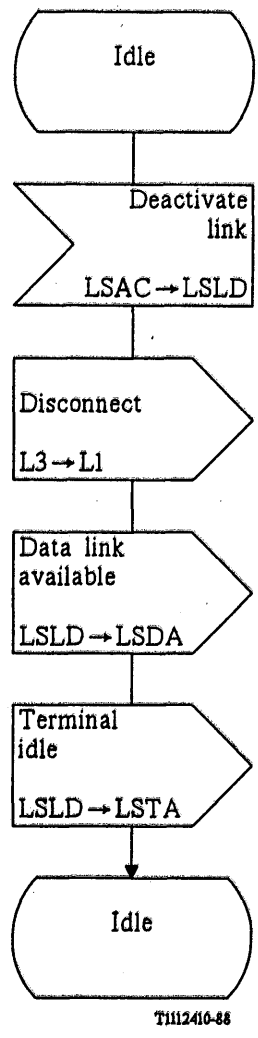



FIGURE 40/Q.704

**Signalling link management; signalling link deactivation (LSLD)**

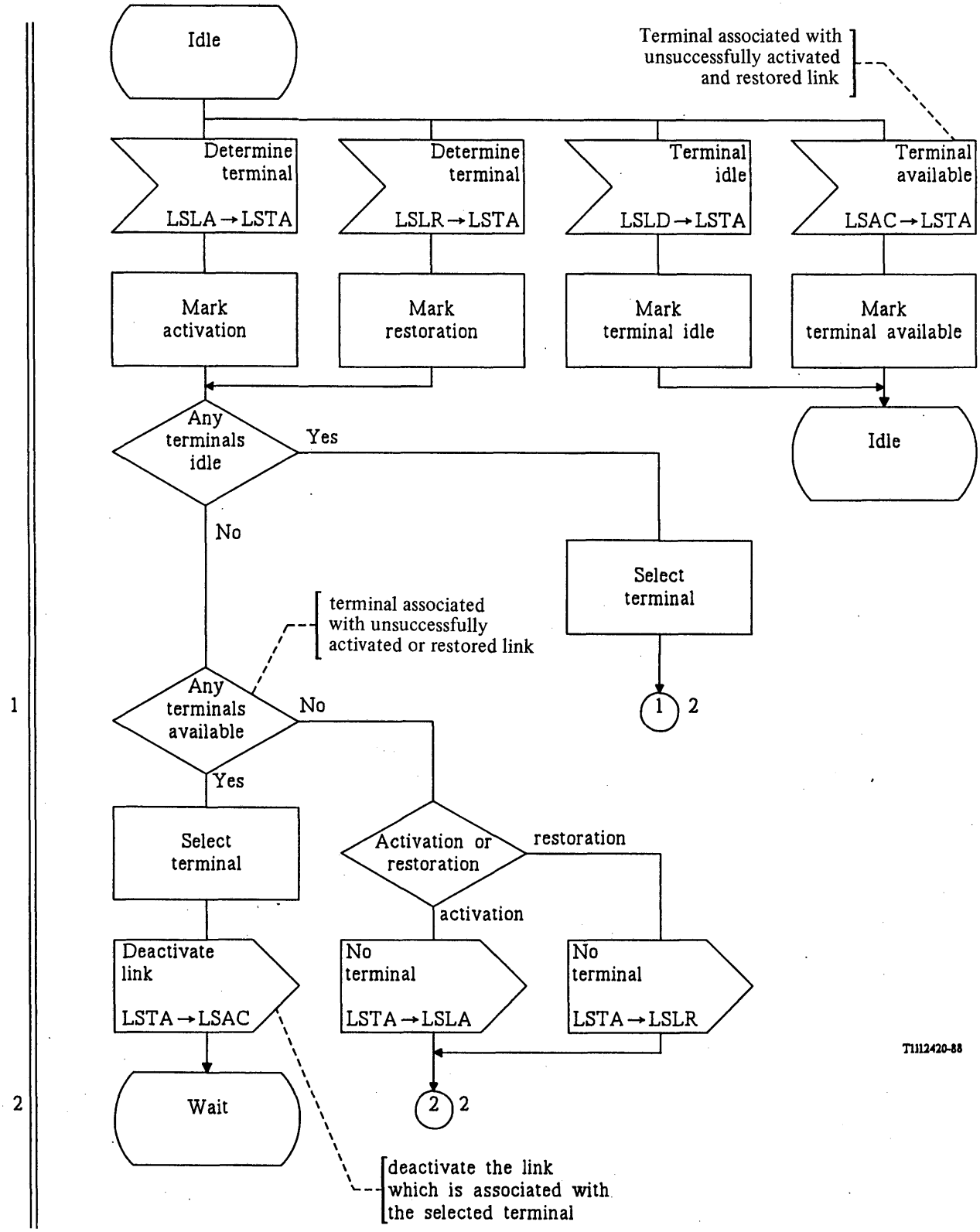



FIGURE 41/Q.704 (sheet 1 of 2)

**Signalling link management; signalling terminal allocation (LSTA)**

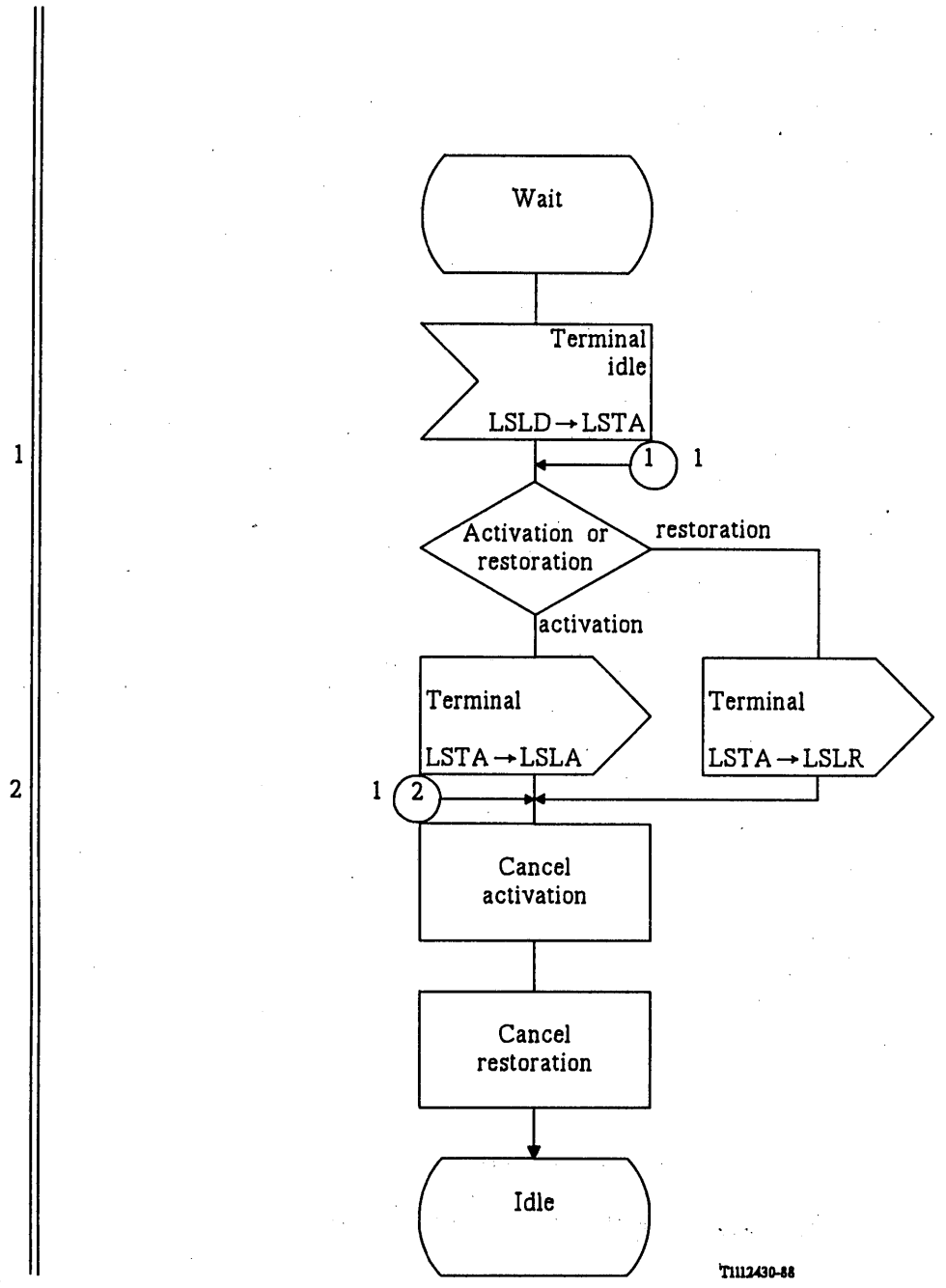



FIGURE 41/Q.704 (sheet 2 of 2)

**Signalling link management; signalling terminal allocation (LSTA)**

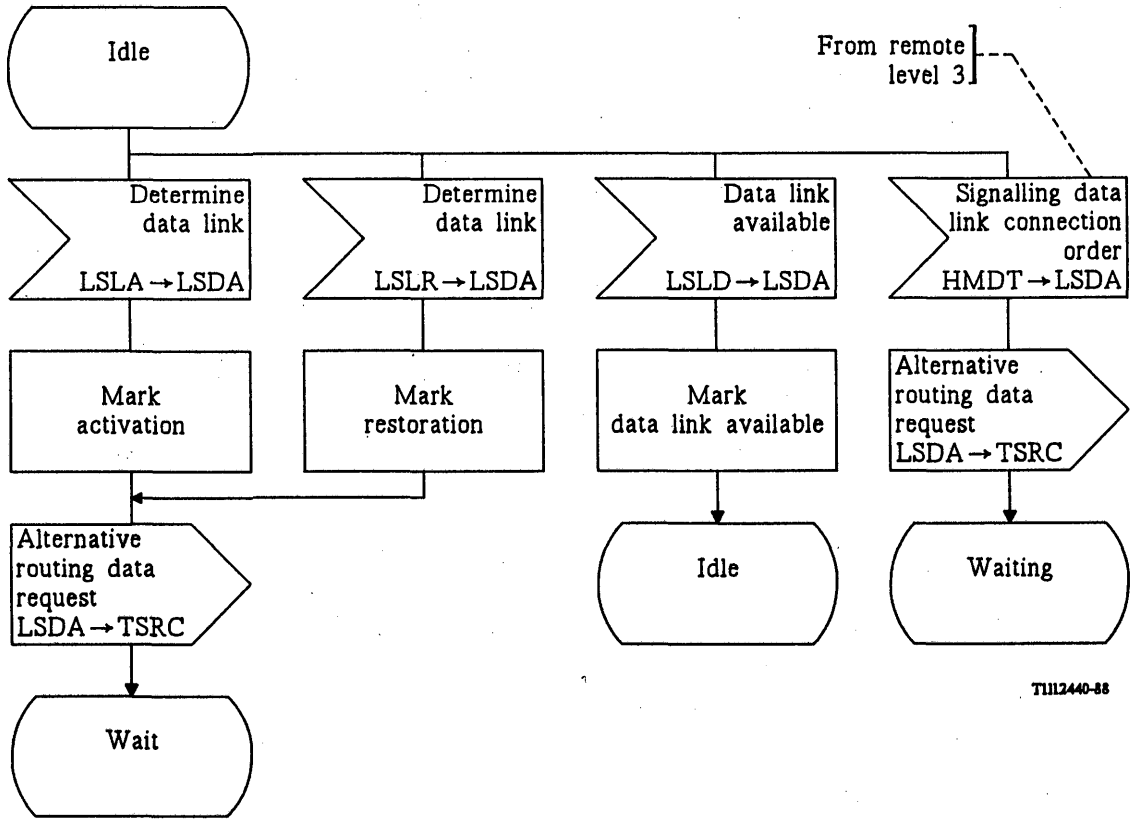



FIGURE 42/Q.704 (sheet 1 of 4)

**Signalling link management; signalling data link allocation (LSDA)**

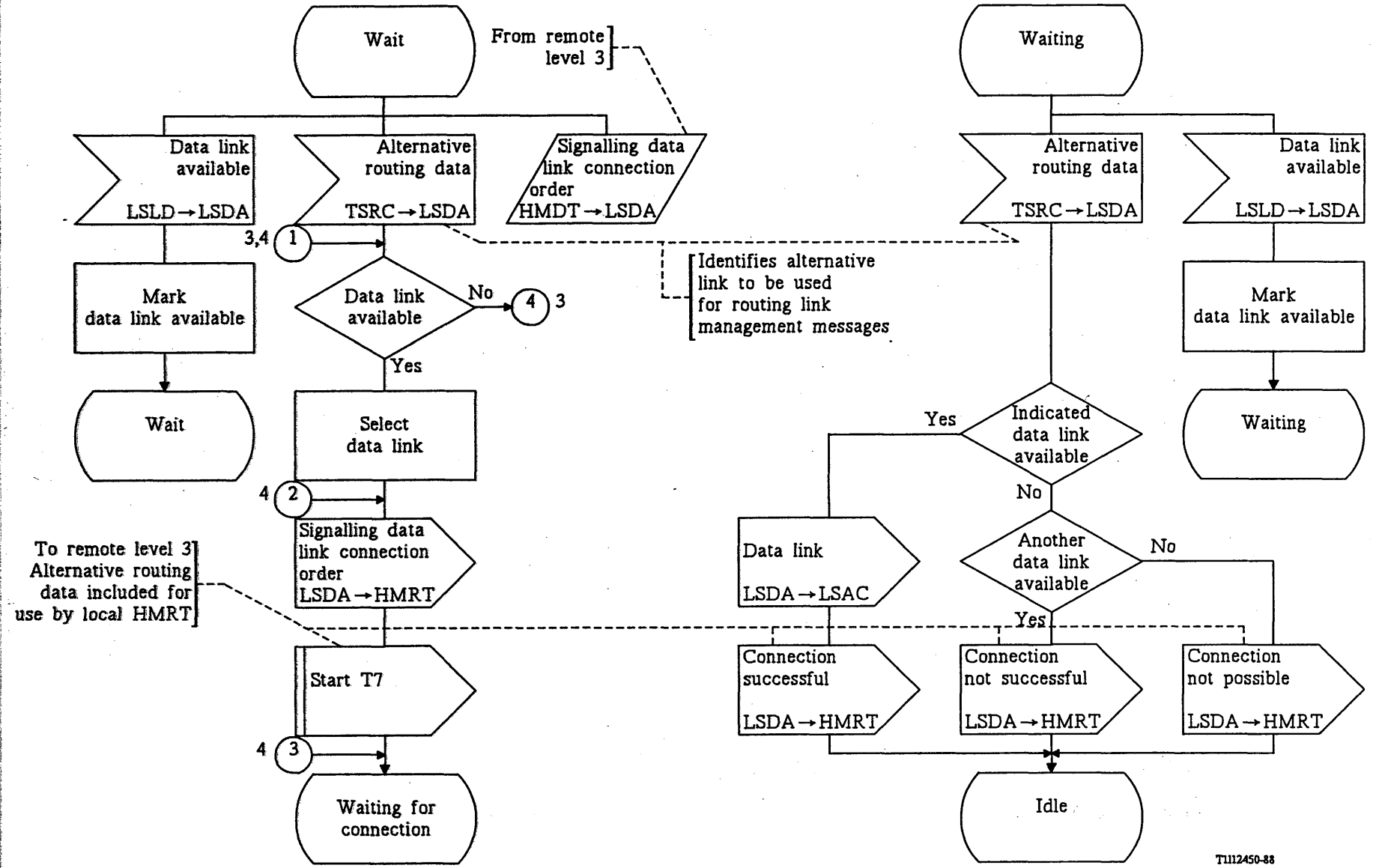



FIGURE 42/Q.704 (sheet 2 of 4)

**Signalling link management; signalling data link allocation (LSDA)**

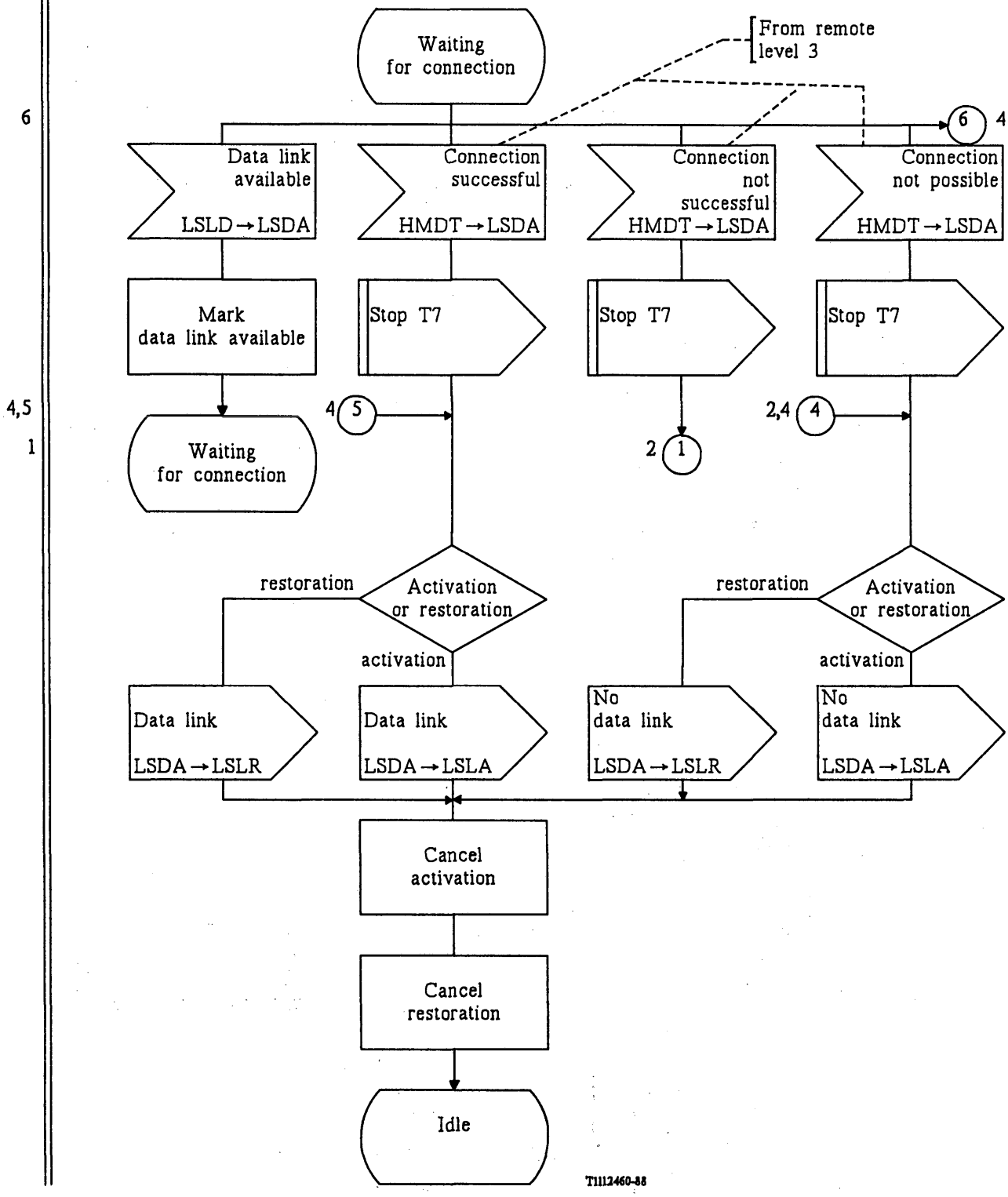



FIGURE 42/Q.704 (sheet 3 of 4)

**Signalling link management; signalling data link allocation (LSDA)**

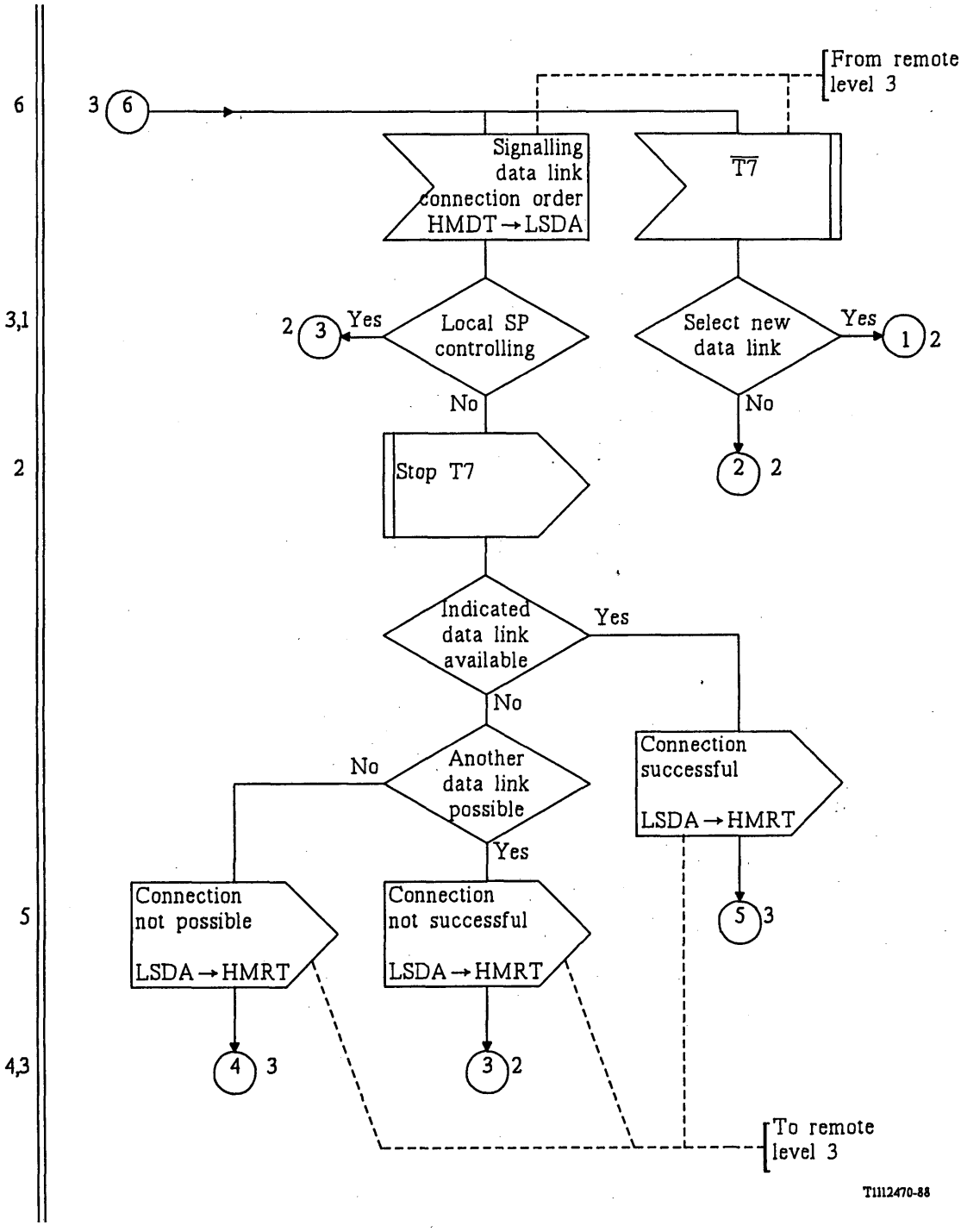
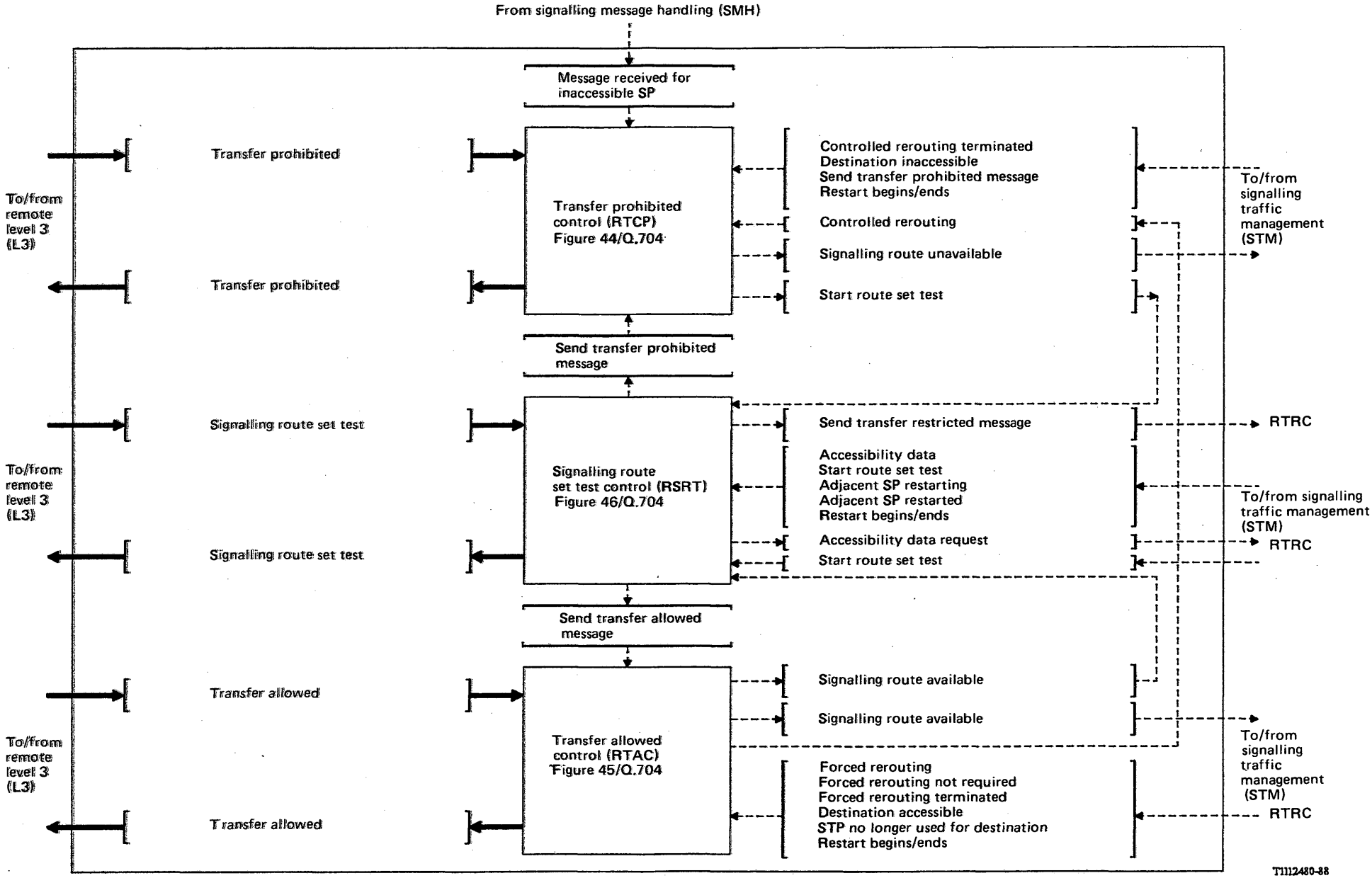



FIGURE 42/Q.704 (sheet 4 of 4)

**Signalling link management; signalling data link allocation (LSDA)**




*Note* – Abbreviated message names have been used in this diagram (i.e. origin – destination codes have been omitted).

FIGURE 43/Q.704 (sheet 1 of 2)

**Level 3 – Signalling route management (SRM); functional block interactions**

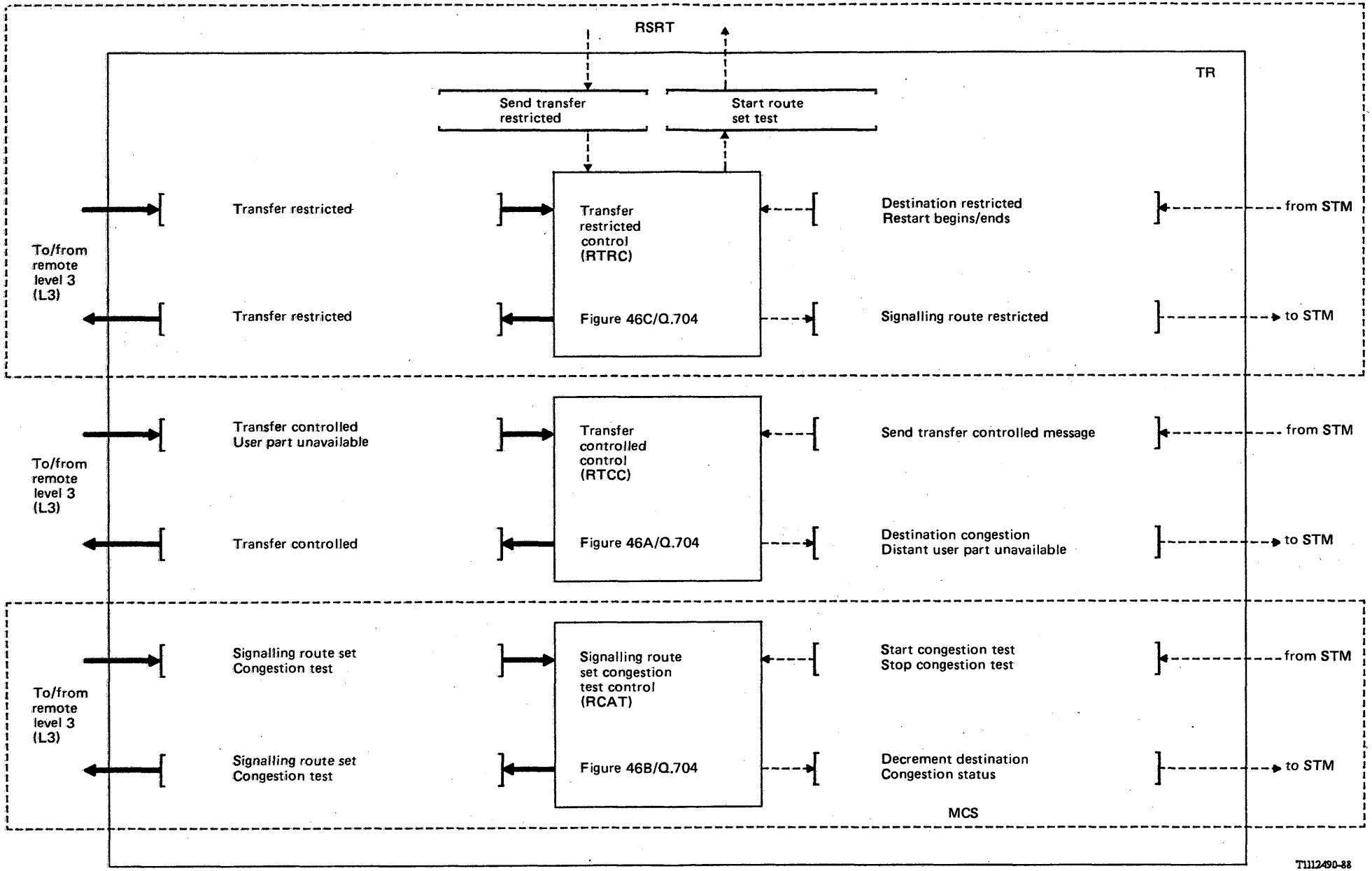



FIGURE 43/Q.704 (sheet 2 of 2)

**Level 3 – Signalling route management (SRM); functional block interactions**

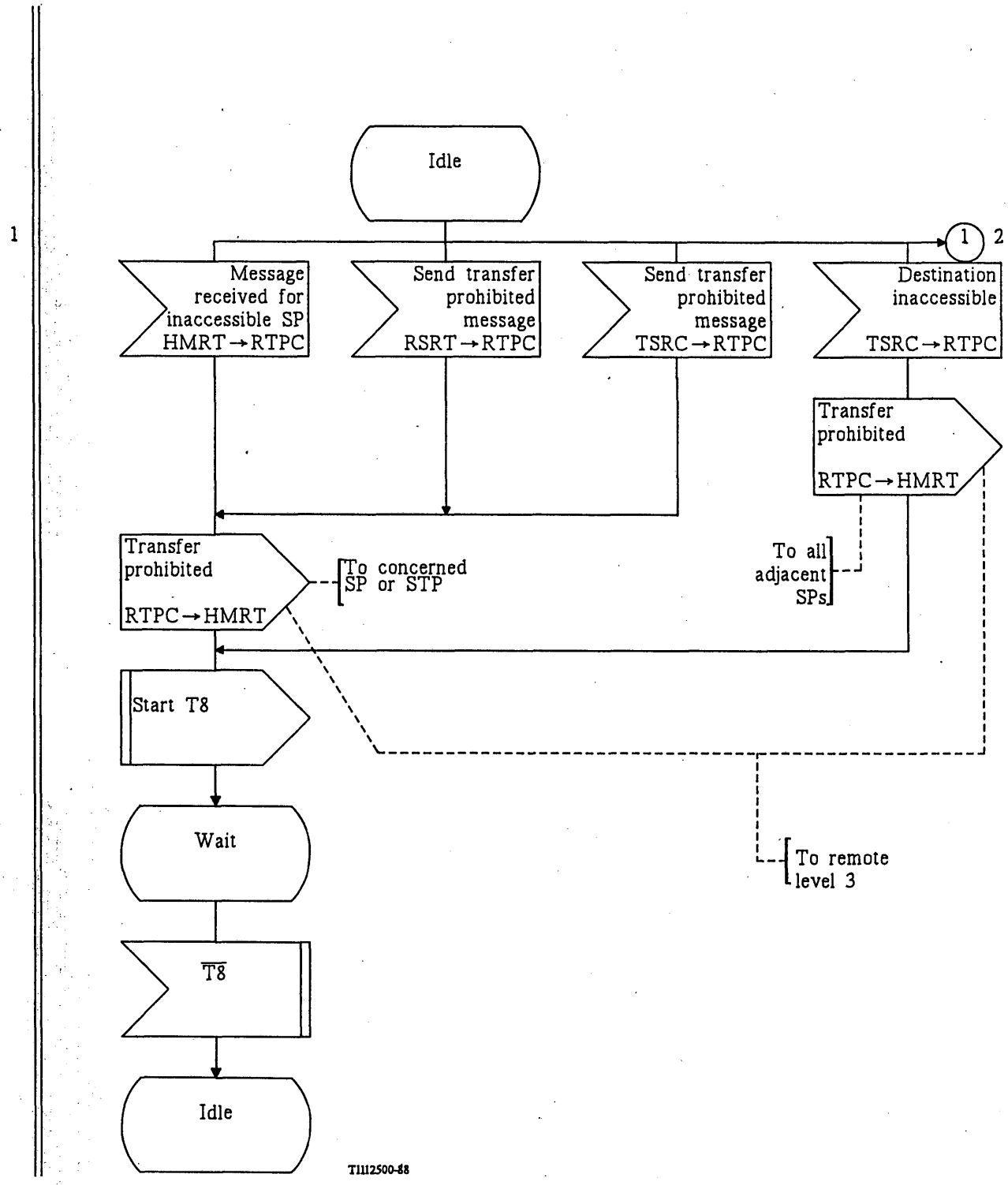



FIGURE 44/Q.704 (sheet 1 of 3)

**Signalling route management; transfer prohibited control (RTPC)**

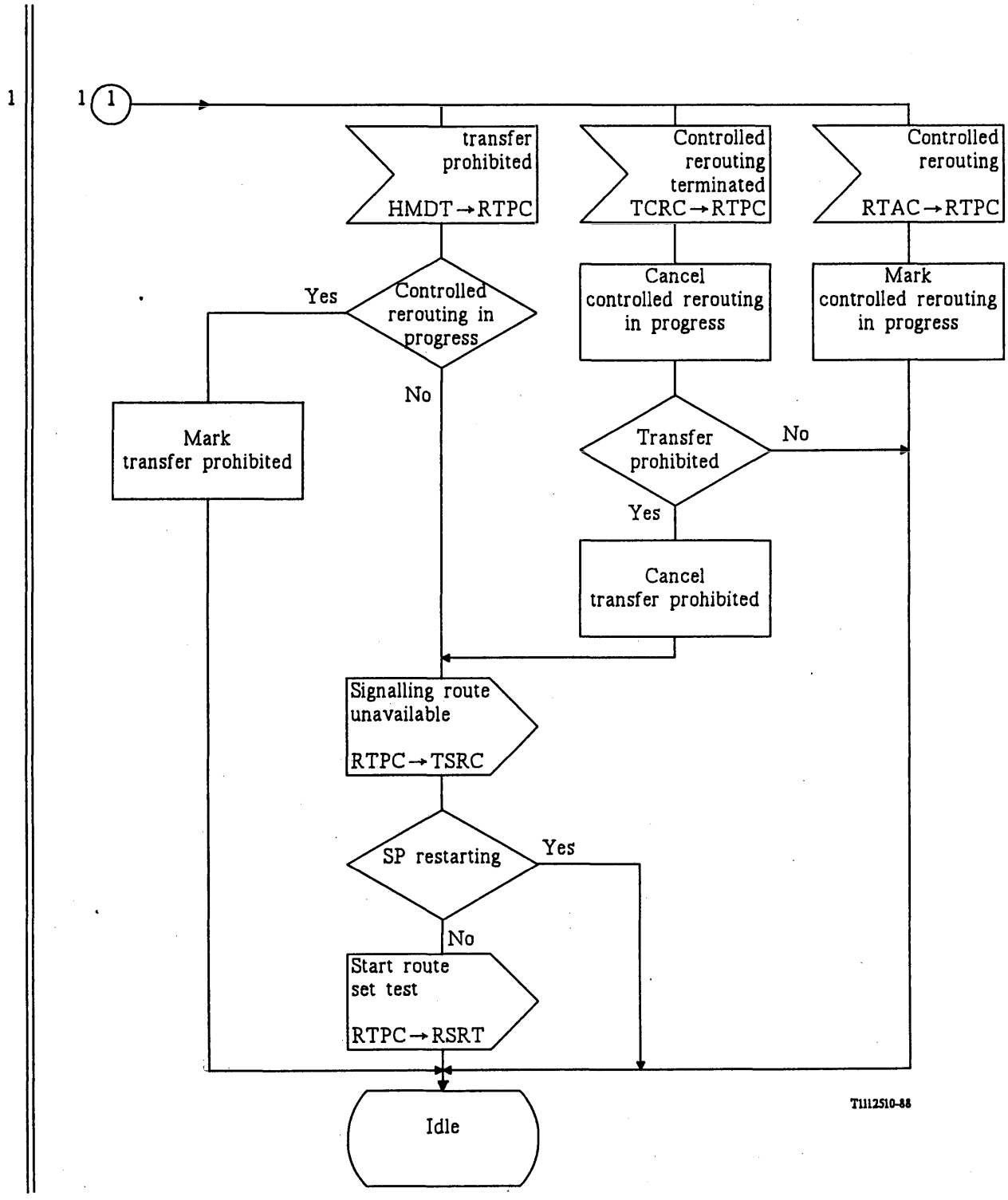



FIGURE 44/Q.704 (sheet 2 of 3)

**Signalling route management; transfer prohibited control (RTPC)**

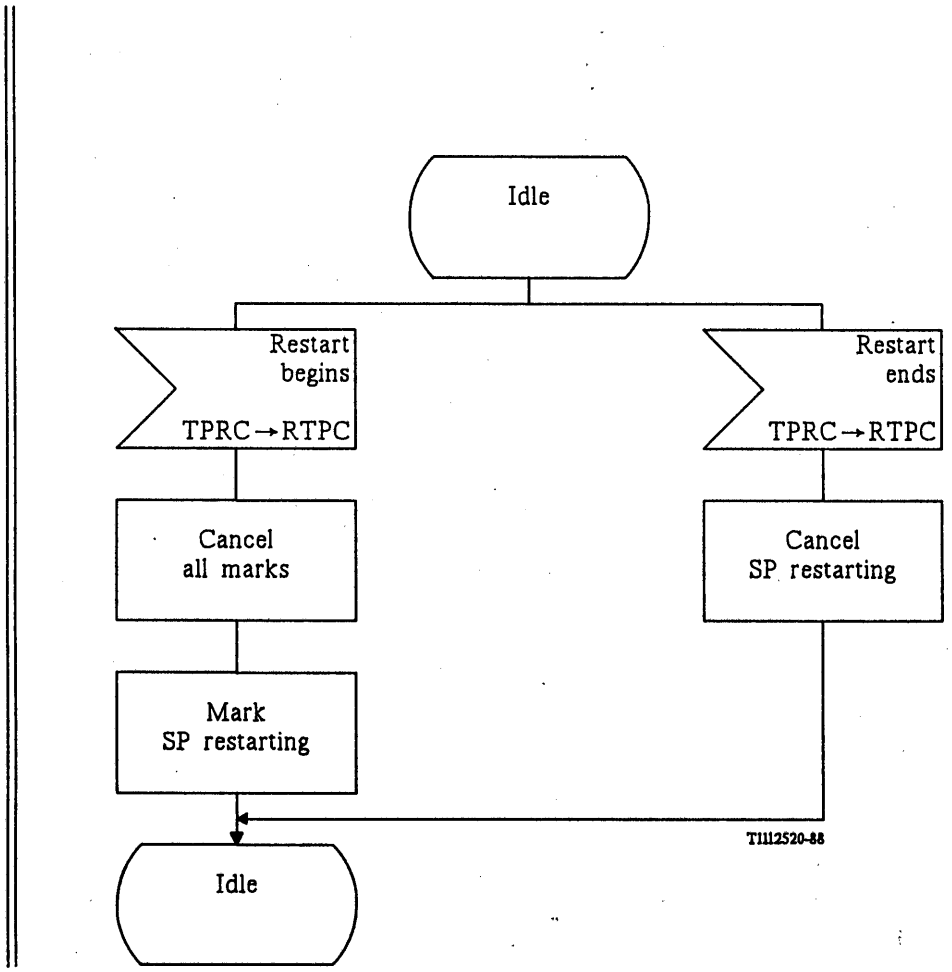



FIGURE 44/Q.704 (sheet 3 of 3)

**Signalling route management; transfer prohibited control (RTPC)**

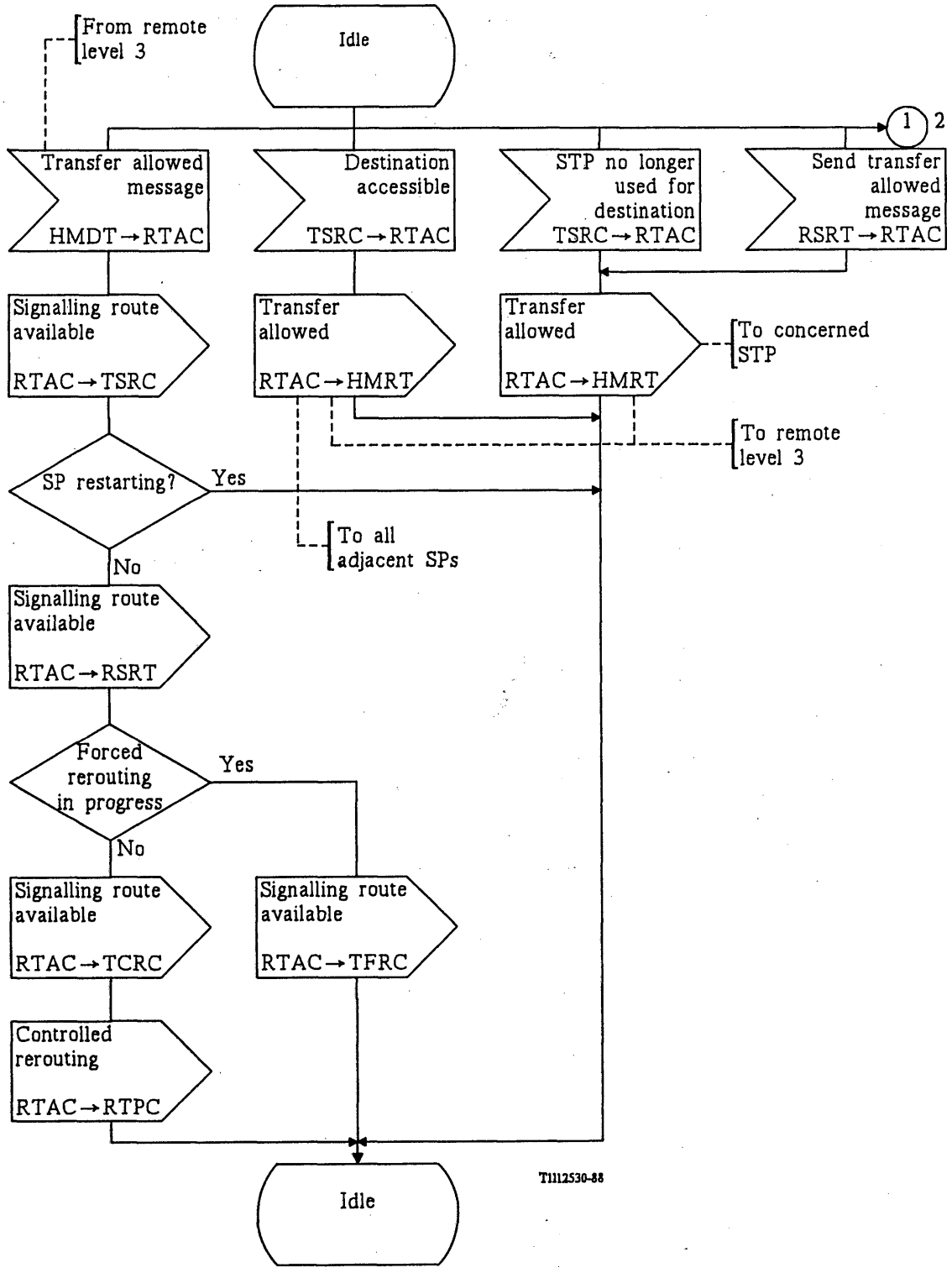



FIGURE 45/Q.704 (sheet 1 of 2)

**Signalling route management; transfer allowed control (RTAC)**

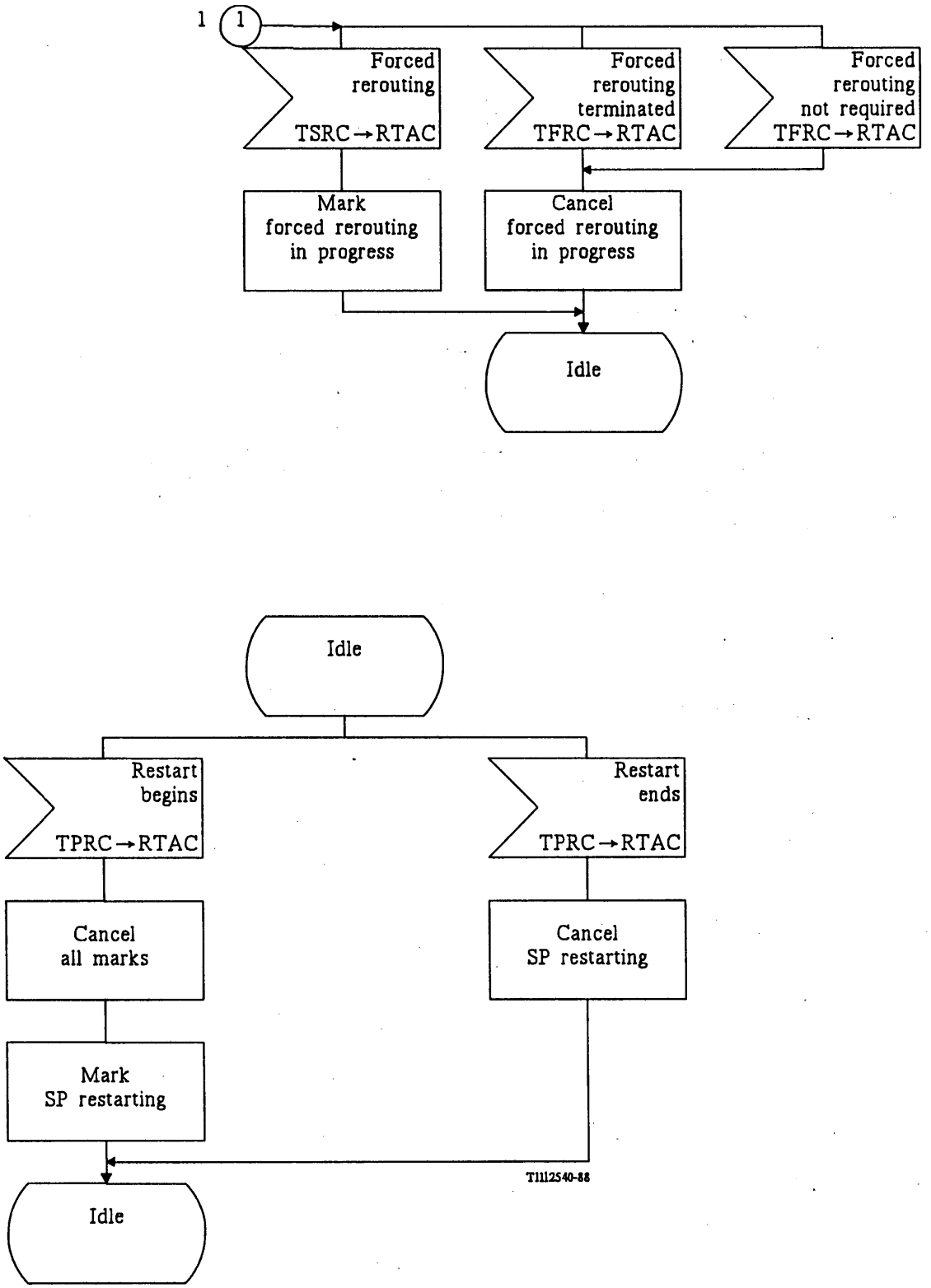
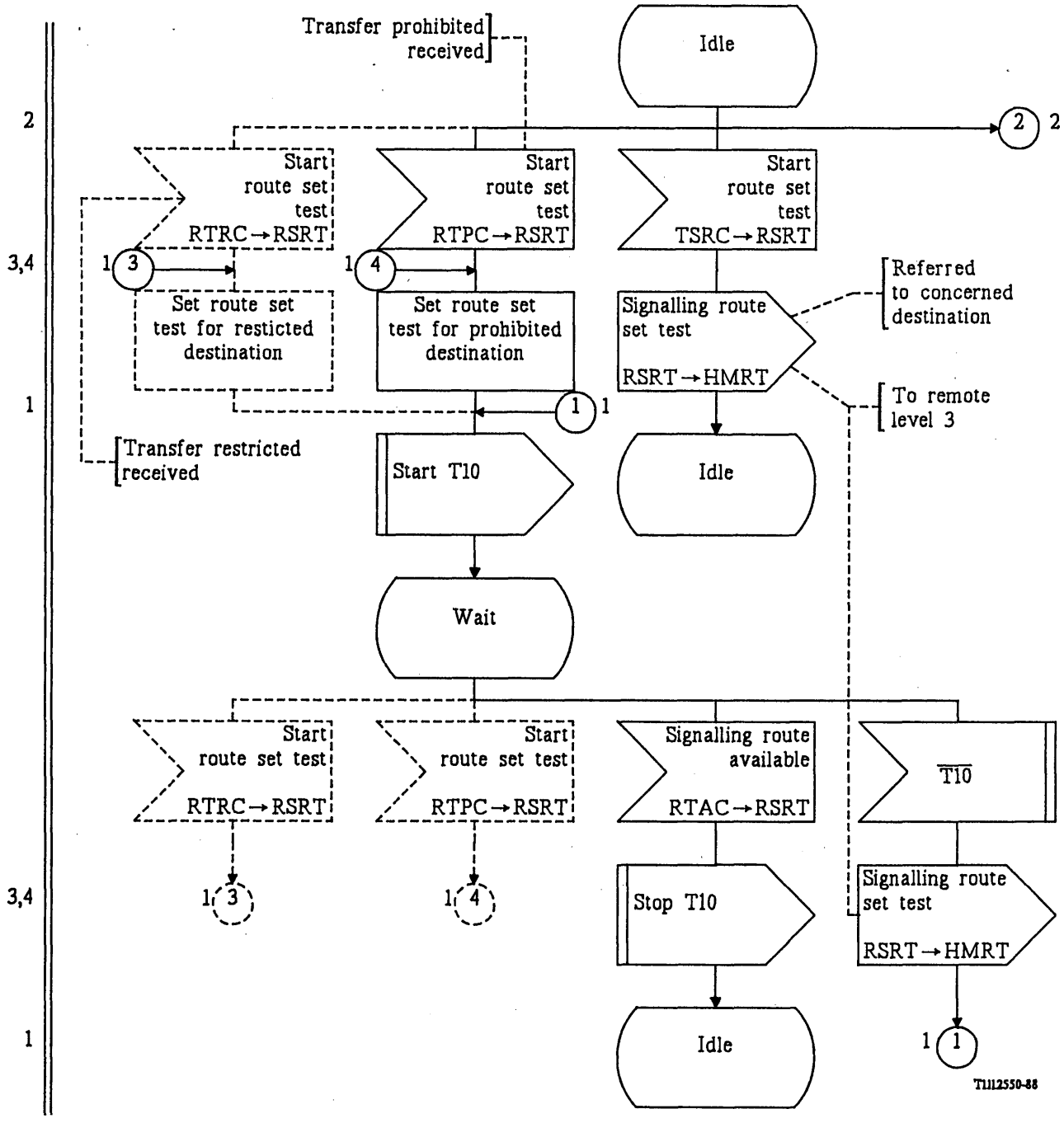



FIGURE 45/Q.704 (sheet 2 of 2)

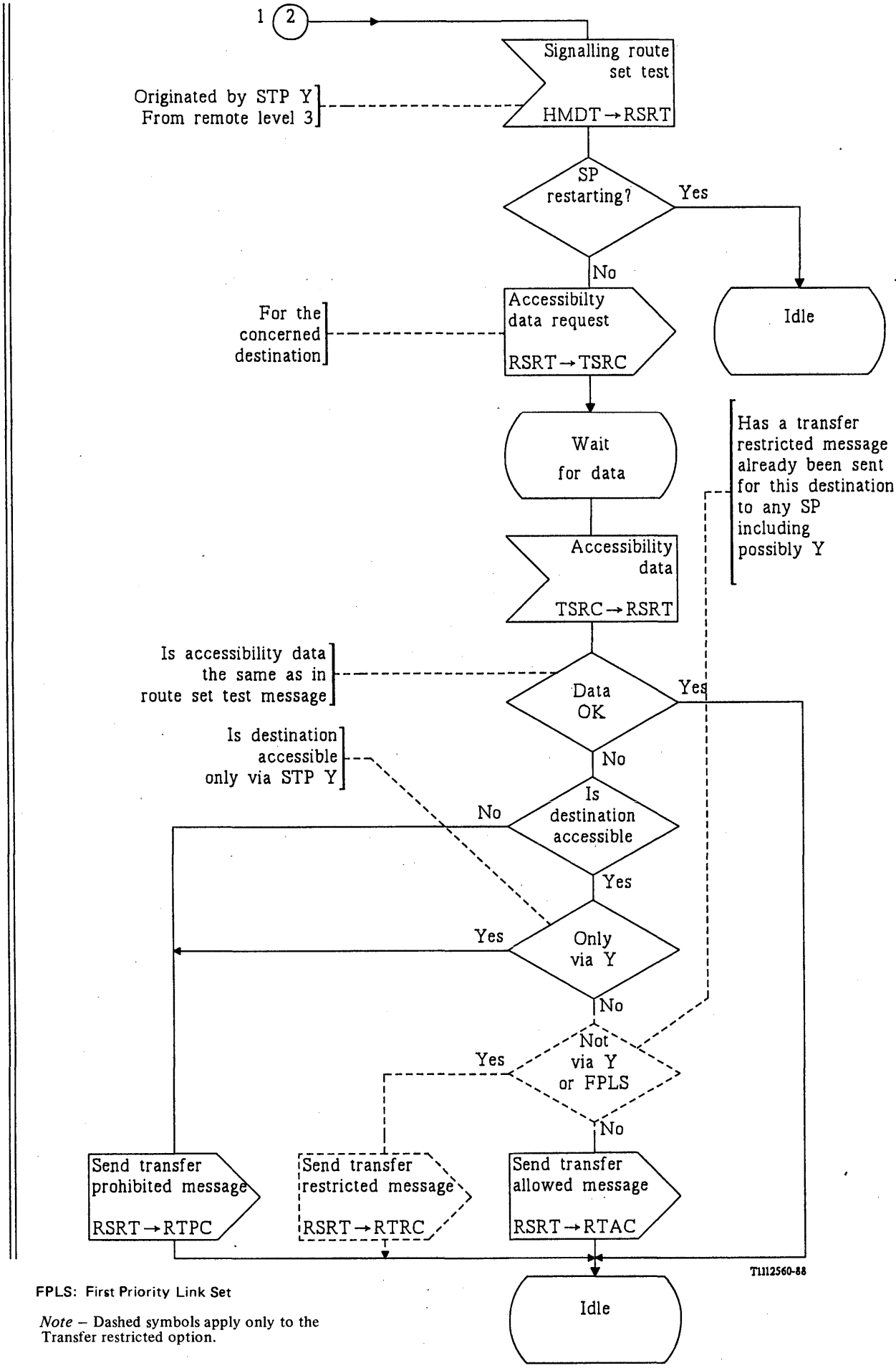
**Signalling route management; transfer allowed control (RTAC)**




*Note* – Dashed symbols apply only to the Transfer restricted option.

FIGURE 46/Q.704 (sheet 1 of 3)

**Signalling route management; signalling route set test control (RSRT)**




FPLS: First Priority Link Set

*Note* – Dashed symbols apply only to the Transfer restricted option.

FIGURE 46/Q.704 (Sheet 2 of 3)

**Signalling route management; signalling route set test control (RSRT)**

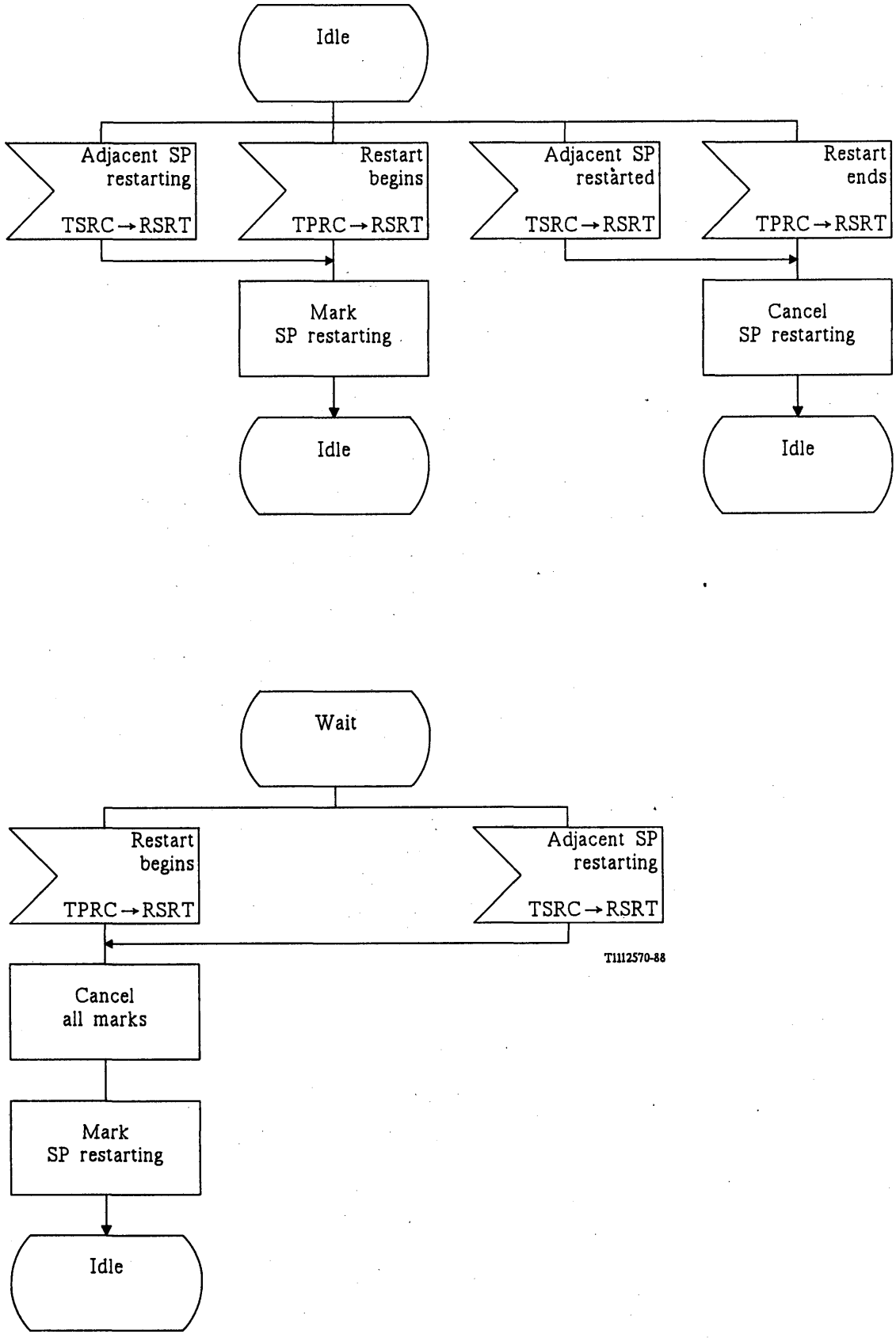
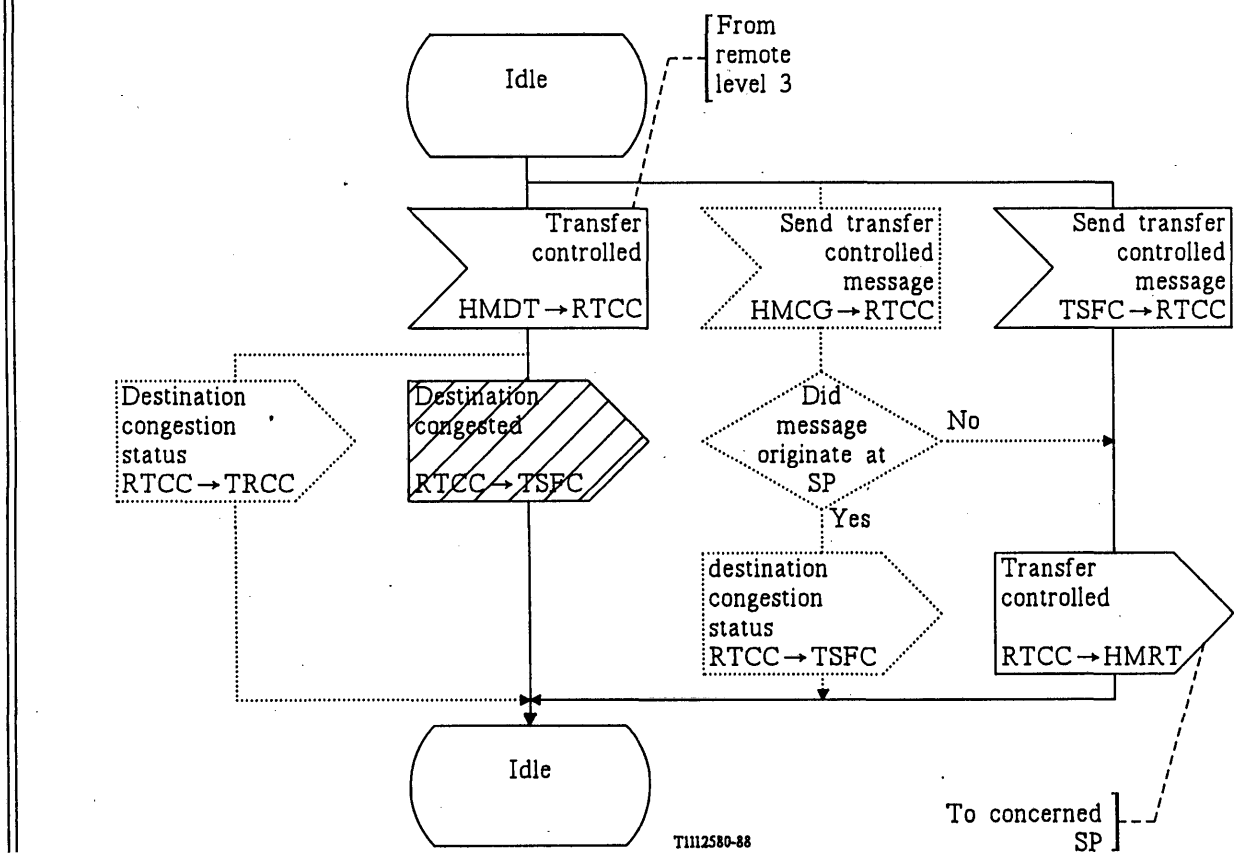



FIGURE 46/Q.704 (sheet 3 of 3)

**Signalling route management; signalling route set test control (RSRT)**




*Note* – Dotted symbols apply only to the multiple congestion states option delete hatched symbols when using option.

FIGURE 46a/Q.704 (sheet 1 of 2)

**Signalling route management; transfer controlled control (RTCC)**

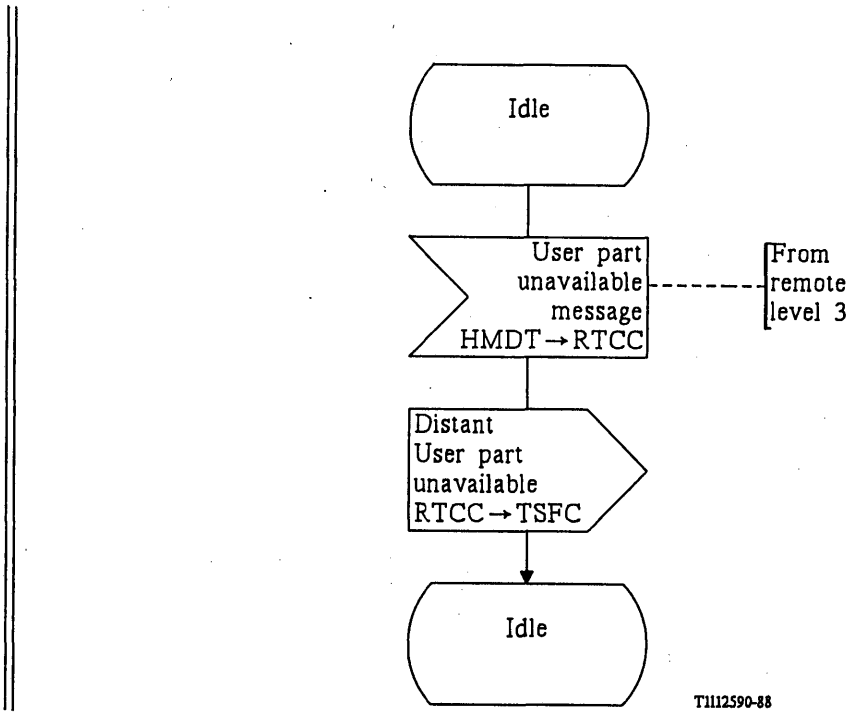
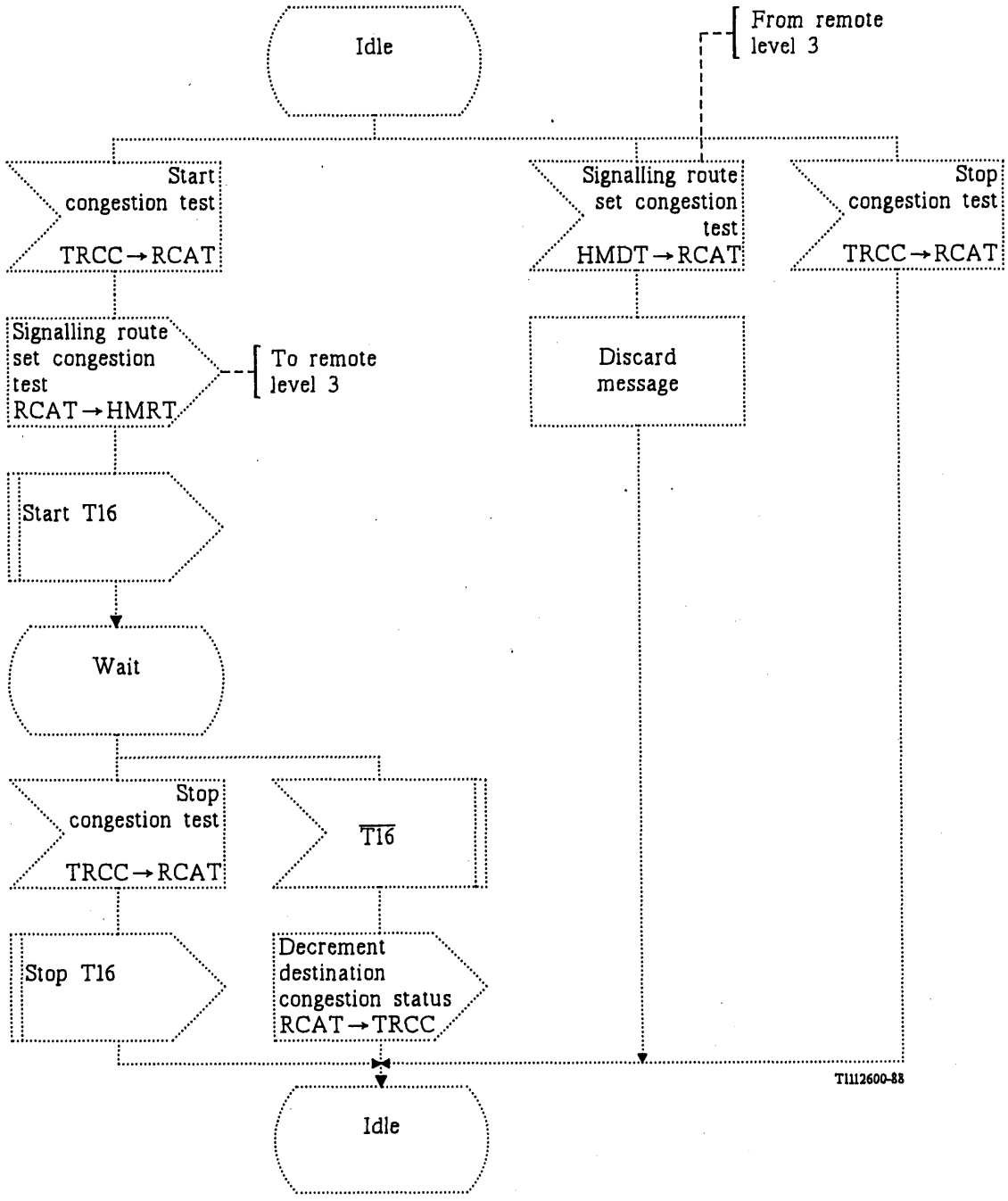



FIGURE 46a/Q.704 (sheet 2 of 2)

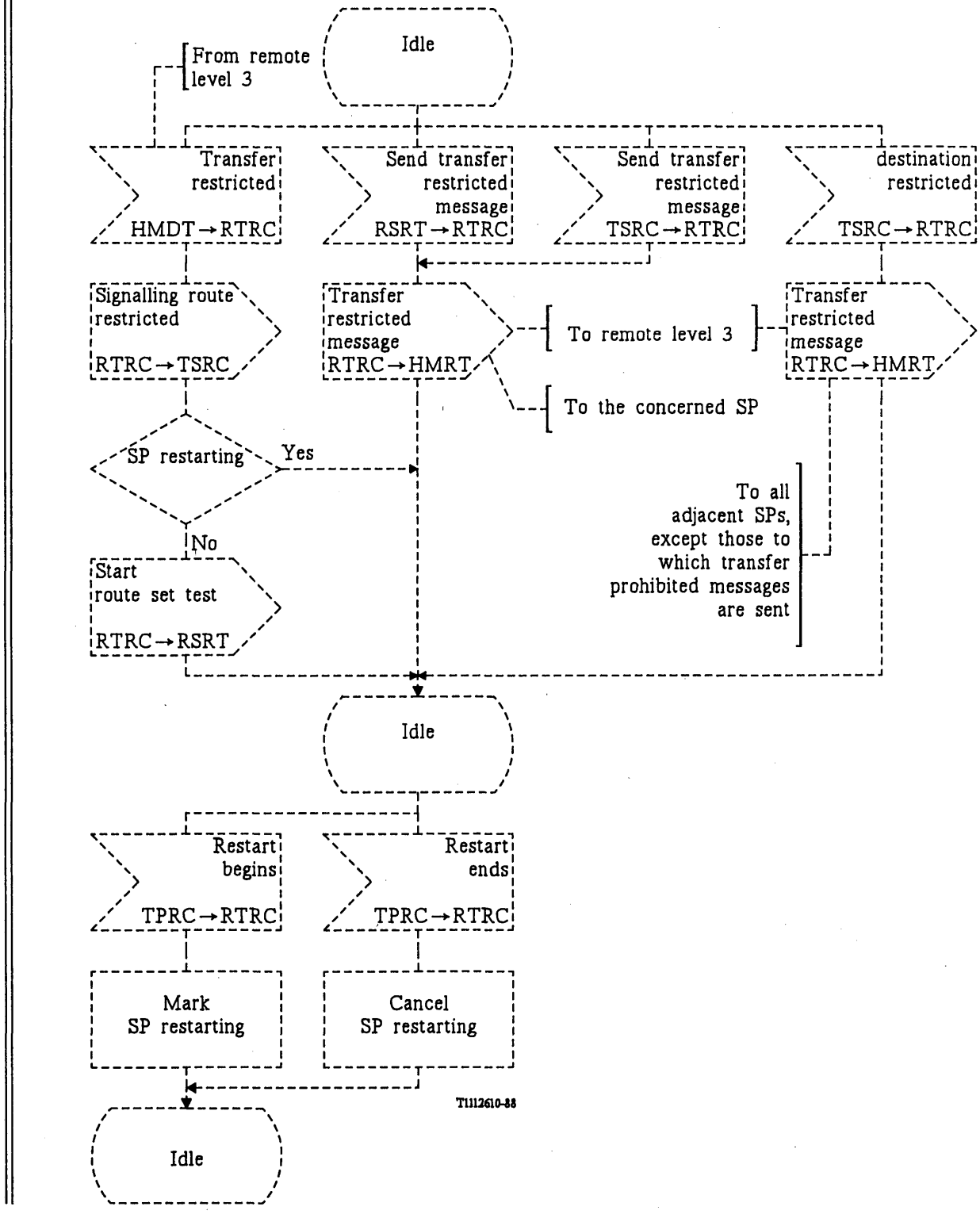
**Signalling route management; transfer controlled control (RTCC)**




*Note* – Dotted symbols apply only to the multiple congestion states option.

FIGURE 46b/Q.704

**Signalling route management; signalling route set congestion test control (RCAT)**




*Note* – Dashed symbols apply only to the Transfer restricted option.

FIGURE 46c/Q.704

**Signalling route management; transfer restricted control (RTRC)**

**Recommendation Q.705**

## SIGNALLING NETWORK STRUCTURE

### 1 Introduction

This Recommendation describes aspects which are pertinent to and should be considered in the design of international signalling networks. Some or all of these aspects may also be relevant to the design of national networks. Some aspects are dealt with for both international and national networks (e.g. availability), others are discussed in the context of the international network only (e.g. number of *signalling transfer points* in a signalling relation). A number of aspects require further study for national networks. This Recommendation also gives in Annex A examples of how the signalling network procedures may be applied to the mesh network representation.

The national and international networks are considered to be structurally independent and, although a particular *signalling point* may belong to both networks, signalling points are allocated *signalling point codes* according to the rules of each network.

The signalling network procedures are provided in order to effectively operate a signalling network having different degrees of complexity. They provide for reliable message transfer across the network and for reconfiguration of the network in the case of failures.

The most elementary signalling network consists of *originating and destination signalling points* connected by a single *signalling link*. To meet availability requirements this may be supplemented by additional links in parallel which may share the signalling load between them. If, for all signalling relations, the originating and destination signalling points are directly connected in this way in a network then the network operates in the *associated mode*.

For technical or economic reasons a simple associated network may not be suitable and a *quasi-associated network* may be implemented in which the information between originating and destination signalling points may be transferred via a number of signalling transfer points. Such a network may be represented by a *mesh network* such as that given in Annex A, as other networks are either a subset of the mesh network or are structured using this network or its subsets as components.

### 2 Network components

#### 2.1 *Signalling links*

Signalling links are basic components in a signalling network connecting together signalling points. The signalling links encompass the *level 2* functions which provide for message error control (detection and subsequent correction). In addition, provision for maintaining the correct message sequence is provided (see Recommendation Q.703).

#### 2.2 *Signalling points*

Signalling links connect signalling points at which signalling network functions such as message routing are provided at *level 3* and at which the user functions may be provided at *level 4* if it is also an originating or destination point (see Recommendation Q.704, § 2.4).

A signalling point that only transfers messages from one signalling link to another at level 3 serves as a signalling transfer point (STP).

The signalling links, signalling transfer points, and signalling (originating or destination) points may be combined in many different ways to form a *signalling network*.

### 3 Structural independence of international and national signalling networks

The worldwide signalling network is structured into two functionally independent levels, namely the international and national levels, as illustrated in Figure 1/Q.705. This structure makes possible a clear division of responsibility for signalling network management and allows numbering plans of signalling points of the international network and the different national networks to be independent of one another.

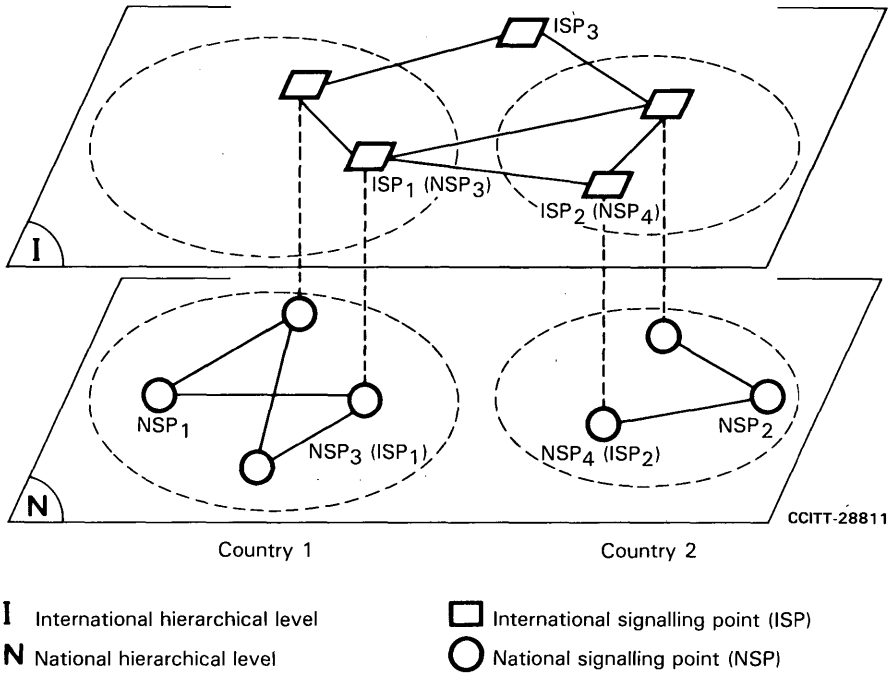



FIGURE 1/Q.705

**International and national signalling networks**

A signalling point (SP), including a signalling transfer point (STP), may be assigned to one of three categories:

- national signalling point (NSP) (signalling transfer point) which belongs to the national signalling network only (e.g. $NSP_1$) and is identified by a signalling point code (OPC or DPC) according to the national numbering plan of signalling points;
- international signalling point (ISP) (signalling transfer point) which belongs to the international signalling network only (e.g. $ISP_3$) and is identified by a signalling point code (OPC or DPC) according to the international numbering plan of signalling points;
- a node that functions both as an international signalling point (signalling transfer point) and a national signalling point (signalling transfer point) and therefore belongs to both the international signalling network and a national signalling network and accordingly is identified by a specific signalling point code (OPC or DPC) in each of the signalling networks.

If a discrimination between international and national signalling point codes is necessary at a signalling point, the network indicator is used (see Recommendation Q.704, § 14.2).

## 4 Considerations common to both international and national signalling networks

### 4.1 *Availability of the network*

The signalling network structure must be selected to meet the most stringent availability requirements of any User Part served by a specific network. The availability of the individual components of the network signalling links, (signalling points, and signalling transfer points) must be considered in determining the network structure (see Recommendation Q.709).

### 4.2 *Message transfer delay*

In order to take account of signalling message delay considerations, regard should be given, in the structuring of a particular signalling network, to the overall number of signalling links (where there are a number of signalling relations in tandem) related to a particular user transaction (e.g., to a specific call in the telephone application) (see Recommendation Q.709).

4.3 *Message sequence control*

For all messages for the same transaction (e.g. a telephone call) the Message Transfer Part will maintain the same routing provided that the same *signalling link selection* code is used in the absence of failure. However, a transaction does not necessarily have to use the same signalling route for both forward and backward messages.

4.4 *Number of signalling links used in load sharing*

The number of signalling links used to share the load of a given flow of signalling traffic typically depends on:

- the total traffic load,
- the availability of the links,
- the required availability of the path between the two signalling points concerned, and
- the bit rate of the signalling links.

Load sharing requires at least two signalling links for all bit rates, but more may be needed at lower bit rates.

When two links are used, each of them should be able to carry the total signalling traffic in case of failure of the other link. When more than two links are used, sufficient reserve link capacity should exist to satisfy the availability requirements specified in Recommendation Q.706.

4.5 *Satellite working*

Due to the considerable increase in overall signalling delay, the use of satellites in Signalling System No. 7 connections requires consideration, and further study is required.

In international operation, when the network served by the signalling network is routed on terrestrial circuits, only in exceptional circumstances should a satellite circuit be employed for the supporting signalling connection.

## 5 International signalling network

5.1 *General*

The international signalling network will use the procedures to be defined in the Signalling System No. 7 Recommendations. The international network structure to be defined can also serve as a model for the structure of national networks.

5.2 *Number of signalling transfer points in signalling relations*

In the international signalling network the number of signalling transfer points between an originating and a destination signalling point should not exceed two in a normal situation. In failure situations, this number may become three or even four for a short period of time. This constraint is intended to limit the complexity of the administration of the international signalling network.

5.3 *Numbering of signalling points*

A 14-bit code is used for the identification of signalling points. The allocation scheme of international signalling point codes is defined in Recommendation Q.708.

5.4 *Routing rules*

5.4.1 In order to ensure full flexibility for the routing of signalling in the System No. 7 international signalling network it appears desirable that at least one signalling point in each country should provide means for the international STP function. Such an approach should ease the use of Signalling System No. 7 on small traffic routes.

5.4.2 *Other routing rules*

(For further study.)

5.5 *Structures*

(Requires further study.)

5.6 *Procedures*

(Requires further study.)

## 6 Signalling network for cross-border traffic

6.1 *General*

For cross-border traffic between signalling points, the need for a special signalling network configuration is identified, because their common interests are such as to generate a considerable volume of traffic between them.

Two alternative arrangements of the signalling network for cross-border traffic are provided so that Administrations may adopt either alternative upon a bilateral agreement.

6.2 *Use of international hierarchical level*

6.2.1 This arrangement could be applied in the case that there are only a relatively small number of signalling points in a country which serve for cross-border traffic.

6.2.2 The signalling points and the signalling transfer points which are involved in a signalling of cross-border traffic should belong to the international hierarchical level described in § 3. When those signalling points or signalling transfer points are also involved in signalling of national traffic, they should belong to their national hierarchical level as well. Therefore the double numbering of signalling point codes based on both the international and national numbering schemes should be required.

6.2.3 A discrimination between international and national point codes is made by the network indicator in the service information octet (see Recommendation Q.704, § 14.2).

6.2.4 Signalling network management procedures in this network arrangement require further study.

6.3 *Integrated numbering of national signalling networks*

6.3.1 By this arrangement the signalling points, which serve cross-border traffic, should be identified by common national signalling point codes.

6.3.2 Common block of national signalling point codes is provided by bilateral agreement (further study is required).

6.4 *Interworking of national signalling networks*

At the cross-border signalling network interface, the international specification of Signalling System No. 7 should be preferred without exclusion of bilateral agreements.

## 7 National signalling network

Any specific structures for national signalling networks are not required to be included in the Recommendation, however, Administrations should cater for requirements imposed on a national network for the protection of international services in terms of network related user requirements such as availability and performance of the network perceived by users, (see Recommendation Q.709).

## 8 Procedures to prevent unauthorized use of an STP (Optional)

8.1 *General*

Administrations may make bilateral agreements to operate SS7 between their networks. These agreements may place restrictions on the SS7 messages authorized for one administration to send to the other. Restrictions could be made, for example, in the interest of network security or as a result of service restrictions. Unauthorized signalling traffic may be, for example, STP traffic for calls set up via networks other than that containing the STP, which has not been agreed bilaterally.

An Administration making an agreement with restrictions may wish to identify and provide special treatment to unauthorized SS7 messages.

The measurements in Table 6/Q.791 provide some capability to identify unauthorized SS7 messages. The procedures in this section for identifying and responding to unauthorized traffic are additional options for use at an STP with signalling links to other networks.

### 8.2 *Identifying unauthorized SS7 messages*

In addition to the normal signalling message handling, procedures specified in Recommendation Q.704, it shall be possible to inhibit/allow messages destined for another signalling point (SP) based on any one or combination of the following options:

i) to inhibit/allow STP access by a combination of designated incoming link sets to designated DPCs;

This combination of DPC/incoming link set shall effectively operate in the form of a single matrix. This matrix shall consist of a maximum of 128 DPCs and a maximum of 64 incoming link sets. (These values are for guidance and may be adjusted to satisfy the requirements of the concerned Operator/Administration.)

ii) To inhibit/allow STP access by a combination of designated outgoing link sets to designated DPCs.

This combination of DPC/outgoing link set shall effectively operate in the form of a single matrix. This matrix shall consist of a maximum of 128 DPCs and a maximum of 64 outgoing link sets. (These values are for guidance and may be adjusted to satisfy the requirements of the concerned Operator/Administration.)

iii) to inhibit/allow STP access by examination of OPC and DPC combination in the incoming STP message.

This combination of DPC/OPC shall effectively operate in the form of a single matrix. This matrix shall consist of a maximum of 128 DPCs and a maximum of 128 OPCs. (These values are for guidance and may be adjusted to satisfy the requirements of the concerned Operator/Administration.)

### 8.3 *Treatment of unauthorized SS7 messages*

An STP identifying unauthorized SS7 messages should be able, on a per link set or per signalling point code basis, to:

i) provide all unauthorized SS7 messages with the same handling as authorized traffic, or

ii) discard all unauthorized SS7 messages.

In addition, an STP should be able to:

i) allow all STP messages outside the designated ranges as given in § 8.2,

ii) bar (discard) all STP messages outside the designated ranges as given in § 8.2.

### 8.4 *Measurements*

An STP identifying unauthorized SS7 messages incoming from another network should be able to count and record details of the unauthorized messages on a per link set and/or signalling point code basis.

### 8.5 *Notification to unauthorized user*

An STP identifying unauthorized SS7 messages from another network may wish to notify the Administration orginating the unauthorized message(s).

This notification should be undertaken by administrative means and not involve any mechanism in Signalling System No. 7.

In addition, a violation fault report shall be issued giving the unauthorized message content. It shall be possible to selectively restrict the number of violation reports on a per link set and/or signalling point code basis.

It shall also be possible to inhibit the violation reporting mechanism on a point code/link set basis, nodally, or on a message direction, i.e. if an inhibited message is destined for an RPOA then it shall be possible to suppress the violation reports whilst allowing violation reports on inhibited messages from the RPOA.

ANNEX A

(to Recommendation Q.705)

**Mesh signalling network examples**

A.1 *General*

This Annex is provided to demonstrate the procedures defined in Recommendation Q.704. While the example uses a specific *mesh* network to demonstrate the procedures, it is not the intent of this annex to recommend either implicitly or explicitly the network described.

The *mesh* network is used to demonstrate the Message Transfer Part level 3 procedures because it is thought to be a possible international network implementation as shown on it, or subsets of it, may be used to construct other network structures.

A.2 *Basic network structures (example)*

Figure A-1/Q.705 shows the basic mesh network structure, while three simplified versions derived from this basic network structure are shown in Figure A-2/Q.705. More complex signalling networks can be built, using these as building components.

In the following, the basic mesh network Figure A-1/Q.705 is taken as an example to explain the procedures defined in Recommendation Q.704.

In this network, each signalling point with level 4 functions is connected by two link sets to two signalling transfer points. Each pair of signalling transfer points is connected to each other pair by four link sets. Moreover, there is a link set between the two signalling transfer points of each pair.

The simplified versions a), b) and c) of the basic signalling network are obtained by deleting respectively:

a) two out of four intersignalling transfer point link sets;

b) link sets between signalling transfer points of the same pair; and

c) a) and b) together.

It should be noted that for a given signalling link availability, the more signalling link sets removed from the basic signalling network [e.g. in going from Figure A-1/Q.705 to Figure A-2c)/Q.705], the lower the availability of the signalling network. However, an increase in the availability of the simplified signalling networks may be attained by adding one or more parallel signalling links to each of the remaining signalling link sets.

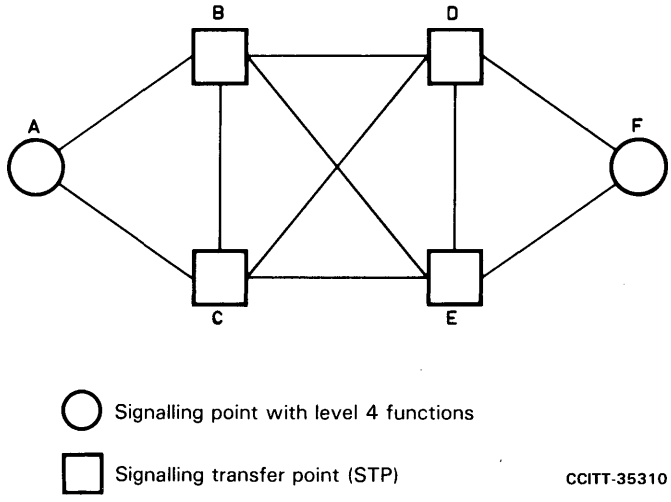
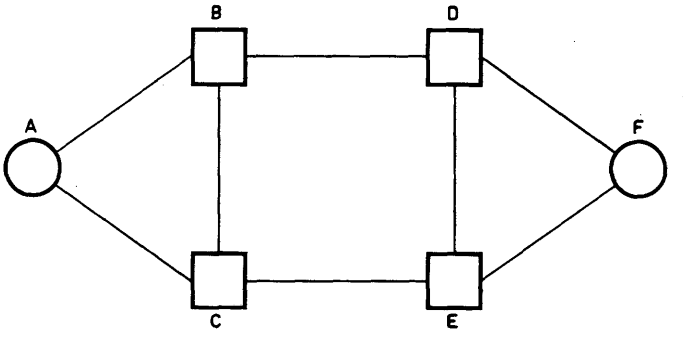
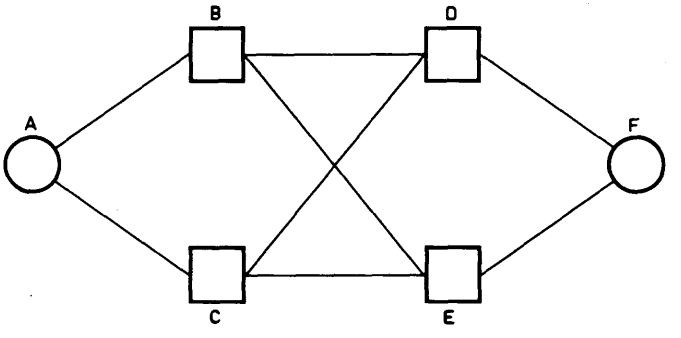



FIGURE A-1/Q.705

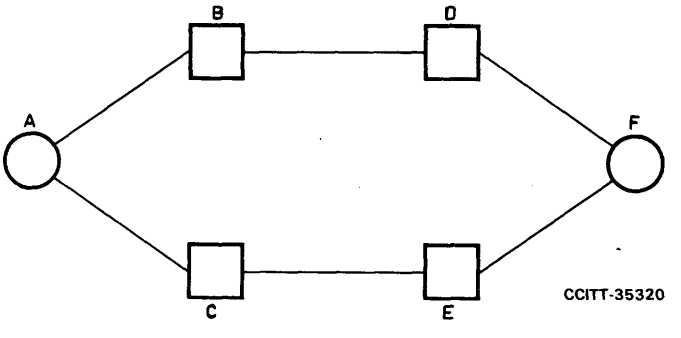
**Basic mesh network**




*a) Two out of four inter-STP link sets deleted*




*b) Link sets between STPs of the same pair deleted*




*c) Two out of four inter-STP link sets and link sets between STPs of the same pair deleted*

FIGURE A-2/Q.705

**Simplified versions of the basic mesh network**

## A.3 *Routing*

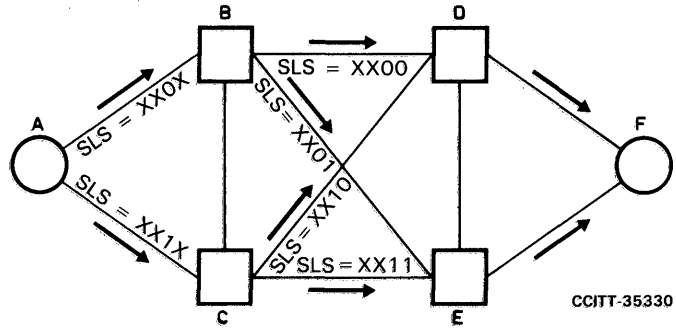
### A.3.1 *General*

This section gives some routing examples in the basic mesh network in Figure A-1/Q.705. Routing actions required to change message routes under failure conditions are described in § A.4. The following routing principles are assumed for the examples in § A.3:

- Message routes should pass through a minimum number of intermediate signalling transfer points.
- Routing at each signalling point will not be affected by message routes used up to the concerned signalling transfer points.
- When more than one message route is available, signalling traffic should be load-shared by such message routes.
- Messages relating to a given user transaction and sent in a given direction will be routed over the same message route to ensure correct message sequence.

### A.3.2 *Routing in the absence of failures*

Figure A-3/Q.705 illustrates an example of routing in the absence of failures for messages from signalling point A to signalling point F.




Normal message routes from A to F

— A → B → D → F (SLS = XX00)
— A → C → D → F (SLS = XX10)
— A → B → E → F (SLS = XX01)
— A → C → E → F (SLS = XX11)

SLS Signalling link selection code in the routing label
Assumption: There is only one link between adjacent signalling points

FIGURE A-3/Q.705

**An example of routing in the absence of failures**

The following points are worthy of note:

a) In distributing traffic for load-sharing at the originating signalling point and intermediate signalling transfer points, care should be taken in the use of signalling link selection (SLS) codes so that traffic will be distributed over four available routes evenly. In the example, originating signalling point A uses the second least significant bit of the signalling link selection code, and signalling transfer points B and C the least significant bit.

b) Other than that described above, the choice of a particular link for a given signalling link selection code can be made at each signalling point independently. As a result, message routes for a given user transaction (e.g. SLS = 0010) in two directions may take different paths (e.g. A → C → D → F and F → E → B → A).

c) Links BC and DE are not used in the absence of failures. They will be used in certain failure situations described in § A.4.

d) When the number of links in a link set is not a power of 2 (i.e. 1, 2, 4, 8), SLS load sharing does not achieve even distribution of traffic across the individual links.

### A.3.3 *Routing under failure conditions*

#### A.3.3.1 *Alternative routing information*

In order to cope with failure conditions that may arise, each signalling point has alternative routing information which specifies, for each normal link set, alternative link set(s) to be used when the former become(s) unavailable (see Recommendation Q.704, § 4.2).

Table A-1/Q.705 gives, as an example, a list of alternative link sets for all normal link sets at signalling point A and at signalling transfer point B. In the basic mesh network, all link sets except those between signalling transfer points of the same pair are normal links which carry signalling traffic in the absence of failures. In case a normal link set becomes unavailable, signalling traffic formerly carried by that link set should be diverted to the alternative link set with priority 1. Alternative link sets with priority 2 (i.e. link sets between signalling transfer points of the same pair) will be used only when both the normal link set and alternative link set(s) with priority 1 become unavailable.

Paragraphs A.3.3.2 to A.3.3.5 present some typical examples of the consequences of faults in signalling links and signalling points on the routing of signalling traffic. For the sake of simplicity, link sets are supposed to consist of only one link each.

TABLE A-1/Q.705

**List of alternative link sets at signalling points A and B**

| | Normal link set | Alternative link set | Priority [a] |
|---|---|---|---|
| Signalling point A | AB | AC | 1 |
| | AC | AB | 1 |
| Signalling transfer point B | BA | BC | 2 |
| | BC | None | |
| | BE | BD | 1 |
| | | BC | 2 |
| | BD | BE | 1 |
| | | BC | 2 |

[a] *Priority 1* – used with normal link set on load-sharing basis in the absence of failures.

*Priority 2* – used only when all the link sets with priority 1 become unavailable.

A.3.3.2 *Single link failure examples*

*Example 1:* Failure of a link between a signalling point and a signalling transfer point (e.g. link AB) (see Figure A-4/Q.705).

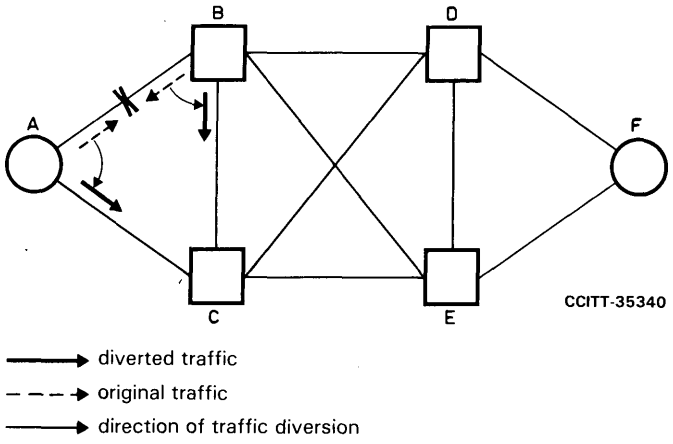



FIGURE A-4/Q.705
**Failure of link AB**

As indicated in Table A-1/Q.705, A diverts traffic formerly carried by link AB to link AC, while B diverts such traffic to link BC. It should be noted that the number of signalling transfer points traversed by signalling messages from F to A which passes through B is increased by one and becomes three in this case.

The principle to minimize the number of intermediate signalling transfer points in § A.3.1 is applied in this case at signalling transfer point B to get around the failure. In fact, the procedures defined in Recommendation Q.704 assume that traffic is diverted at a signalling point only in the case of a signalling link being unavailable on the route outgoing from that signalling point. Therefore, the procedures do not provide for sending an indication that traffic routed via signalling transfer point B will traverse a further signalling transfer point.

*Example 2:* Failure of an intersignalling transfer points link (e.g. link BD) (see Figure A-5/Q.705).

As indicated in Table A-1/Q.705, B diverts traffic carried by link BD to link BE. In the same sense, D diverts traffic carried by link DB to link DC.

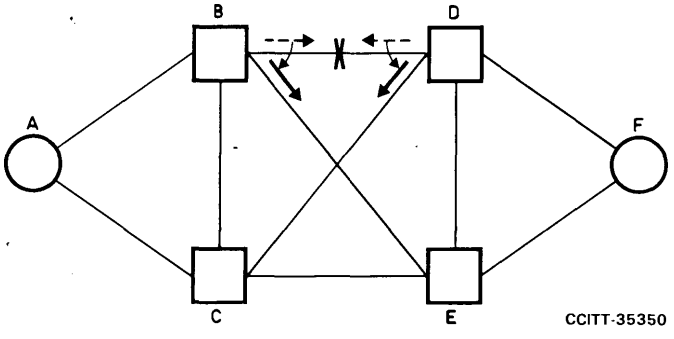



FIGURE A-5/Q.705
**Failure of link BD**

*Example 3:* Failure of a link between signalling transfer points of the same pair (e.g. link BC) (see Figure A-6/Q.705).

No routing change is required as a result of this kind of failure. Only B and C take note that the link BC has become unavailable.

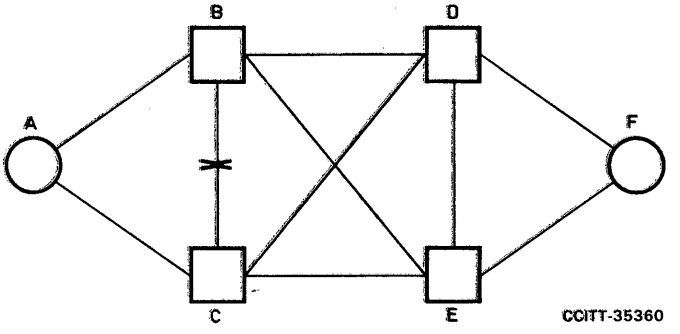



FIGURE A-6/Q.705
**Failure of link BC**

A.3.3.3 *Multiple link failure examples*

As there are a variety of cases in which more than one link set becomes unavailable, only some typical cases are given as examples in the following.

*Example 1:* Failure of a link between a signalling point and a signalling transfer point, and of the link between that signalling transfer point and that of the same pair (e.g. links DF, DE) (see Figure A-7/Q.705).

B diverts traffic destined to F from link BD to link BE, because destination F becomes inaccessible via D. It should be noted that only the traffic destined to F is diverted from link BD to link BE, and not all the traffic on link BD. The same applies to C, which diverts traffic destined to F from link CD to link CE. F diverts all the traffic formerly carried by link FD to link FE in the same way as the single link failure example in § A.3.3.2.

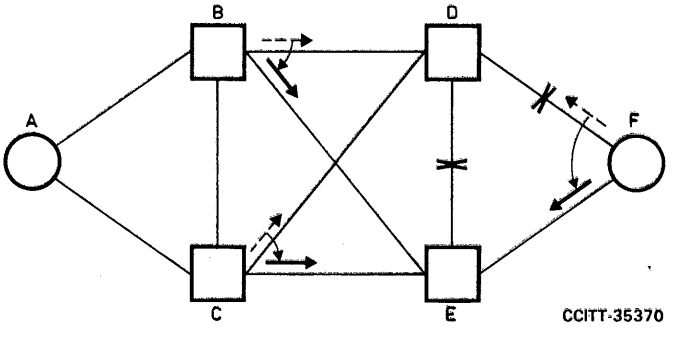



FIGURE A-7/Q.705
**Failure of links DE and DF**

*Example 2:* Failure of two intersignalling transfer point links (e.g. links BD, BE) (see Figure A-8/Q.705).

B diverts traffic formerly carried by link BD to link BC, because its alternative link set with priority 1, i.e. link BE, is also unavailable. The same applies to traffic formerly carried by link BE, and B diverts it to link BC. D and E divert traffic formerly carried by links DB and EB respectively to links DC and EC in the same way as the single link failure example in § A.3.3.2.

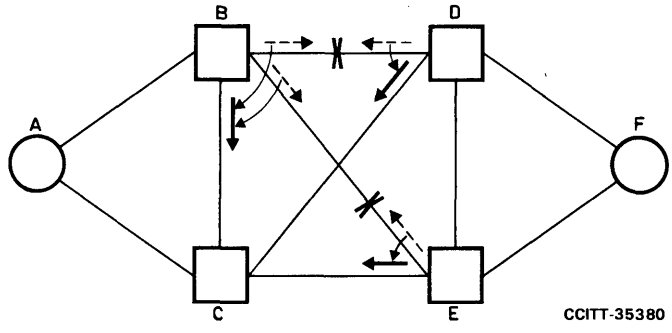



FIGURE A-8/Q.705

**Failure of links BD and BE**

*Example 3:* Failure of a link between a signalling point and a signalling transfer point, and of an intersignalling transfer point link (e.g. links DF and BD) (see Figure A-9/Q.705).

This example is a combination of Examples 1 and 2 in § A.3.3.2. D diverts traffic formerly carried by link DF to link DE, while F diverts it to link FE. Moreover D diverts traffic formerly carried by link DB to link DC (this traffic will be that generated by signalling points other than F connected to D). In the same sense, B diverts traffic carried by link BD to link BE.

It should be noted that in this case only the portion of traffic sent by C to F via D traverses three signalling transfer points (C, D and E), while all the other portions continue to traverse two.

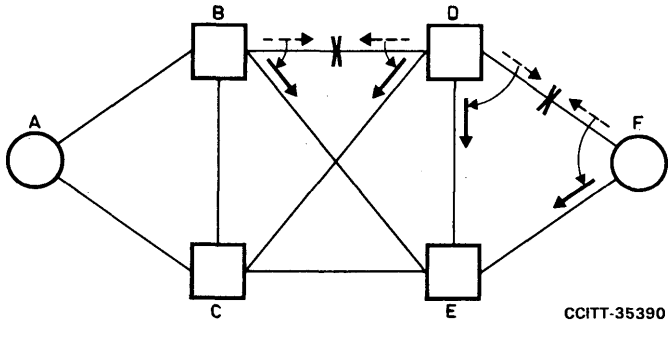



FIGURE A-9/Q.705

**Failure of links BD and DF**

*Example 4:* Failure of the two links between a signalling point and its signalling transfer points (e.g. DF and EF) (see Figure A-10/Q.705).

In this case the signalling relations between F and any other signalling point of the network are blocked. Therefore F stops all outgoing signalling traffic, while A stops only traffic destined to F.

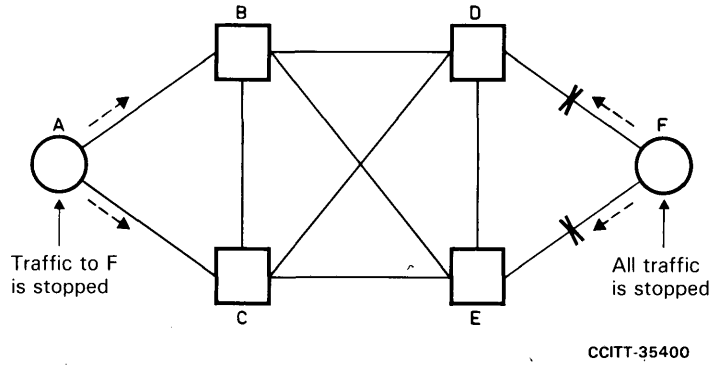



FIGURE A-10/Q.705

**Failure of links DF and EF**

A.3.3.4 *Single signalling point failure examples*

*Example 1:* Failure of a signalling transfer point (e.g. D) (see Figure A-11/Q.705).

B diverts all the traffic formerly carried by link BD to link BE. The same applies to C which diverts all the traffic carried by link CD to link CE. Originating point F diverts all the traffic carried by link FD to link FE as in the case of the link FD failure (see Example 1 in § A.3.3.2).

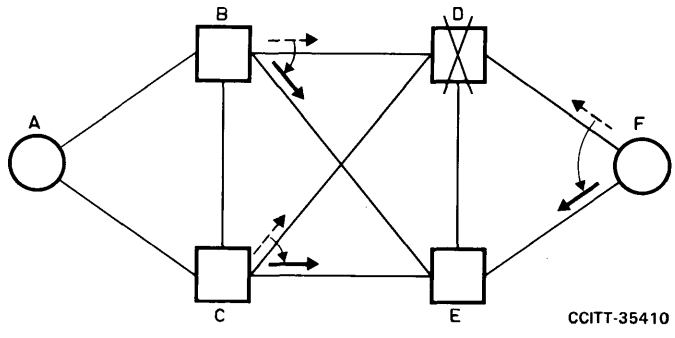



FIGURE A-11/Q.705

**Failure of signalling transfer point D**

Attention is drawn to the difference to Example 1 in § A.3.3.3 where only a part of the traffic previously carried by links BD and CD was diverted.

*Example 2:* Failure of a destination point (e.g. F) (see Figure A-12/Q.705).

In this case A stops all the traffic to F formerly carried on links AB and AC.

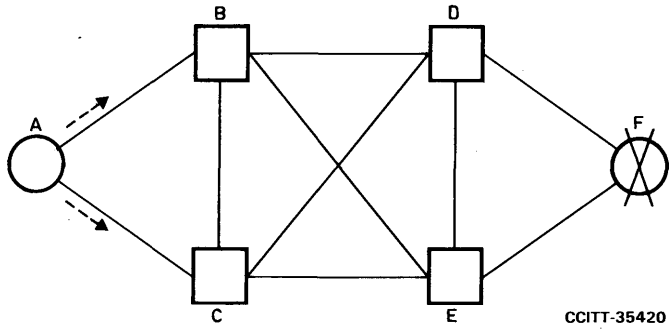



FIGURE A-12/Q.705

**Failure of signalling point F**

A.3.3.5 *Multiple signalling transfer point failure examples*

Two typical cases of two signalling transfer points failing together are presented in the following examples.

*Example 1:* Failure of two signalling transfer points not pertaining to the same pair (e.g. B and D) (see Figure A-13/Q.705).

As a result of the failure of B, A diverts traffic formerly carried by link AB to link AC, while E diverts traffic formerly carried by link EB to link EC. Similarly as a result of the failure of D, F diverts traffic formerly carried by link FD to link FE, while C diverts traffic formerly carried by link CD to link CE.

It should be noted that, in this example, all the traffic between A and F is concentrated on only one intersignalling transfer point link, since failure of a signalling transfer point has an effect similar to a simultaneous failure of all the signalling links connected to it.

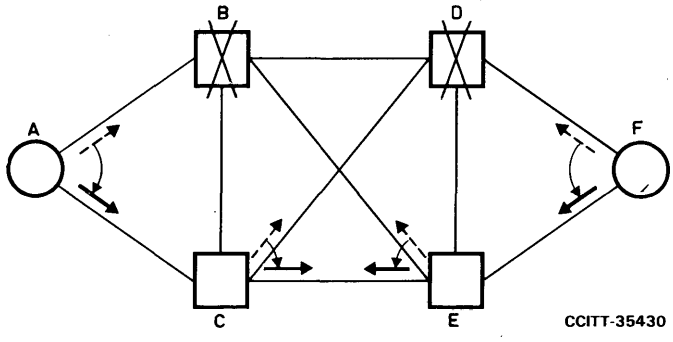



FIGURE A-13/Q.705

**Failure of signalling transfer points B and D**

*Example 2:* Failure of two signalling transfer points pertaining to the same pairs (e.g. D and E) (see Figure A-14/Q.705).

This example is equivalent to Example 4 in § A.3.3.3 as far as the inaccessibility of F is concerned, but in this case any other signalling point connected by its links to D and E also becomes inaccessible. In this case A stops signalling traffic destined to F, while F stops all outgoing signalling traffic.

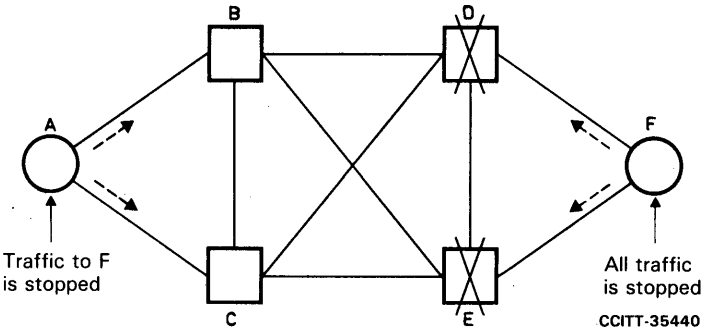



FIGURE A-14/Q.705

**Failure of signalling transfer points D and E**

## A.4 *Actions relating to failure conditions*

In the following, four typical examples of the application of signalling network management procedures to the failure cases illustrated in § A.3.3 are shown. In the case of multiple failures, an arbitrary failure (and restoration) sequence is assumed for illustrative purpose.

### A.4.1 *Example 1: Failure of a link between a signalling point and a signalling transfer point (e.g. link AB)* (see Figure A-15/Q.705)

(Same as § A.3.3.2, Example 1.)

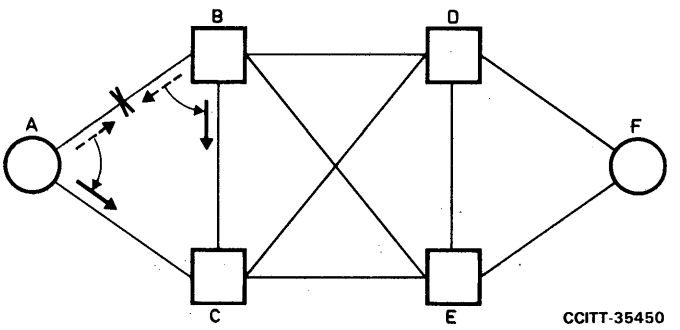



FIGURE A-15/Q.705

**Failure of link AB**

A.4.1.1 *Failure of link AB*

a) When the failure of link AB is detected in A and in B, they initiate the changeover procedure, by exchanging changeover messages via C. Once buffer updating is completed, A restarts the traffic originally carried by the failed link on link AC; similarly, B restarts traffic destined to A on link BC.

b) In addition, B sends a transfer-prohibited message to C referred to destination A (according to the criterion indicated in Recommendation Q.704, § 13.2.2).

c) On the reception of the transfer-prohibited message, C starts the periodic sending of signalling-route-set-test messages, referred to A, to B (see Recommendation Q.704, § 13.5.2).

A.4.1.2 *Restoration of link AB*

When the restoration of link AB is completed, the following applies:

a) B initiates the changeback procedure, by sending a changeback declaration to A via C. Once it has received the changeback acknowledgement, it restarts traffic on the restored link. Moreover, it sends to C a transfer-allowed message, referred to destination A (see Recommendation Q.704, § 13.3.2). When C receives the transfer-allowed message, it stops sending signalling-route-set-test messages to B.

b) A initiates the changeback procedure, by sending a changeback declaration to B via C; once it has received the changeback acknowledgement, it restarts traffic on the normal link. The only traffic to be diverted is that for which link AB is the normal link set according to the load sharing rule (see § A.3.3.1). It must be pointed out, however, that if there is load sharing on parallel links between B and C, there is the possibility of missequencing. Concerning b), for example, the changeback declaration sent from A to B via C might overrun messages still buffered at signalling point C (due to e.g. retransmissions on the parallel link CB).

A.4.2 *Example 2: Failure of signalling transfer point D* (see Figure A-16/Q.705)

(Same as § A.3.3.4, Example 1.)

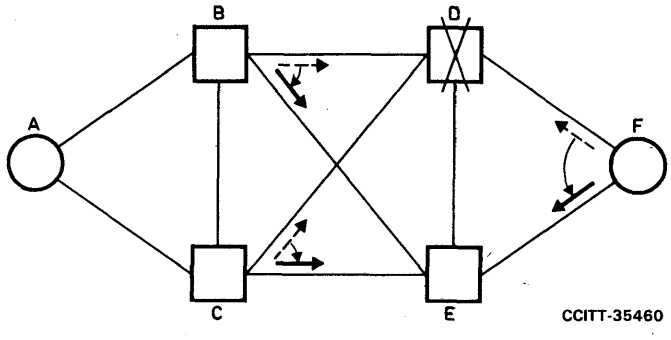



FIGURE A-16/Q.705

**Failure of signalling transfer point D**

A.4.2.1 *Failure of signalling transfer point D*

a) Changeover is initiated at signalling points B, C and F from blocked links BD, CD and FD to the first priority alternative links BE, CE and FE respectively. Due to the failure of D, the concerned signalling points will receive no changeover acknowledgement message in response, and therefore they will restart traffic on alternative links at the expiry of the time T2 (see Recommendation Q.704, § 5.7.2). In addition E will send to B, C and F transfer-prohibited messages referred to destination D. These signalling points (B, C and F) will thus start periodic sending to E of signalling-route-set-test messages referred to D.

b) When B receives a transfer-prohibited message from E referred to D, it updates its routing information so that traffic to D will be diverted to C, thus sending a transfer-prohibited message to C referred to D. The same applies to C, and C sends a transfer-prohibited message to B.

c) So, when B receives a transfer-prohibited message from C, it finds that destination D has become inaccessible and sends a transfer-prohibited message to A. The same applies to C and thus C also sends a transfer-prohibited message to A. Having received transfer-prohibited messages from both B and C, A recognizes that D has become inaccessible and stops traffic to D.

d) In the same manner, i.e. link-by-link transmission of transfer-prohibited messages referred to D, other signalling points B, C, E and F will finally recognize that destination D has become inaccessible. Each signalling point will, therefore, start periodic sending of signalling-route-set-test messages referred to D to their respective adjacent signalling points.

A.4.2.2 *Recovery of signalling transfer point D*

a) Signalling points B, C, E send traffic restart allowed messages to signalling point D, as soon as signalling point D becomes accessible.

b) Signalling transfer point D broadcasts traffic restart allowed messages, after T20 (see Recommendation Q.704, § 16.8) has stopped or expired, to all adjacent SPs.

c) Changeback at signalling points B, C and F from the alternative to their normal links is performed. In all the three cases changeback includes the time-controlled diversion procedure (see Recommendation Q.704, § 6.4), since D is still inaccessible via E at B, C and F (as a result of previous reception of transfer-prohibited message from E).

d) E sends to B, C and F transfer-allowed messages referred to destination D. These signalling points will thus send transfer allowed messages to their respective adjacent signalling points. Thus, the link-by-link transmission of transfer-allowed messages will declare to all signalling points that destination D has become accessible.

e) On reception of a transfer-allowed message, each signalling point stops periodic sending of signalling-route-set-test messages to their respective adjacent signalling points.

f) On recovery of the previously unavailable links BD, CD and FD, signalling points B, C and F will restart all the traffic normally routed via signalling transfer point D after T21 (see Recommendation Q.704, § 16.8) has stopped or expired. (They would restart any traffic terminating at D, if D had an endpoint function as well as being an STP, immediately D becomes accessible, that is after successful signalling link tests to D.)

A.4.3 *Example 3: Failure of link between a signalling point and a signalling transfer point, and of the link between that signalling transfer point and that of the same pair (e.g. links DF, DE)* (see Figure A-17/Q.705)

(Same as § A.3.3.3, Example 1.)

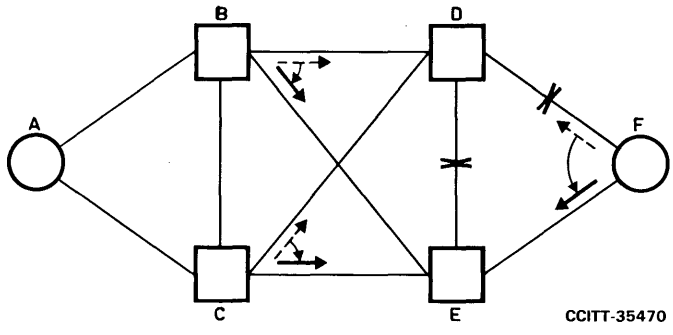



FIGURE A-17/Q.705

**Failure of links DE and DF**

A.4.3.1 *Failure of link DE*

On failure of link DE, this link is marked unavailable at both signalling transfer points D and E. Since in the absence of failures, link DE does not carry signalling traffic, no change in message routing takes place at this time.

However, D and E send to signalling points B, C and F transfer-prohibited messages referred to destination E or D respectively. These signalling points will thus start periodic sending of signalling-route-set-test messages, referred to D or E, to E and D respectively.

A.4.3.2 *Failure of link DF in the presence of failure of link DE*

a) On failure of link DF the following actions occur:
   i) Signalling point D which no longer has access to signalling point F indicates this condition to signalling transfer points B and C by sending transfer-prohibited messages. B and C will thus start the periodic sending of signalling-route-set-test messages referred to F, to D.
   ii) Emergency changeover from link FD to link FE is initiated at signalling point F, since D becomes inaccessible to F due also to the previous failure.

b) On receiving the transfer-prohibited messages forced rerouting is initiated at points B and C. This causes traffic destined to F to be diverted from links terminating on D to links terminating on E. Forced rerouting thus permits recovery from a failure condition caused by a fault in a remote part of the network.

A.4.3.3 *Restoration of link FD in the presence of failure of link DE*

a) On recovery of link FD the following actions occur:
   i) Signalling point D sends a transfer-allowed message to B and C to indicate that D once again has access to F. B and C will thus stop the sending of signalling-route-set-test messages referred to F to D.
   ii) F initiates changeback with time controlled diversion from link FE to link FD. This procedure permits changeback to be executed at one end of a link, when it is impossible to notify the other end of the link (in this example, because link DE is unavailable). Traffic in this case is not diverted from the alternative link until a time interval has elapsed, in order to minimize the danger of mis-sequencing of messages (see Recommendation Q.704, § 6.4).

b) On receiving the transfer-allowed message, controlled rerouting of traffic from the alternative routes (BEF, CEF) to the normal routes (BDF, CDF) is initiated at points B and C. Controlled rerouting involves diversion of traffic to a route which has become available after a time interval (see Recommendation Q.704, § 8.2.1), provisionally set at one second to minimize the danger of mis-sequencing messages.

A.4.3.4 *Restoration of link DE*

On recovery of link DE it is marked available at signalling transfer points D and E. Signalling points D and E send to B, C and F transfer-allowed messages referred to destination E or D respectively. These signalling transfer points will thus stop sending of signalling-route-set-test messages.

A.4.4 *Example 4: Failure of links DF and EF* (see Figure A-18/Q.705)

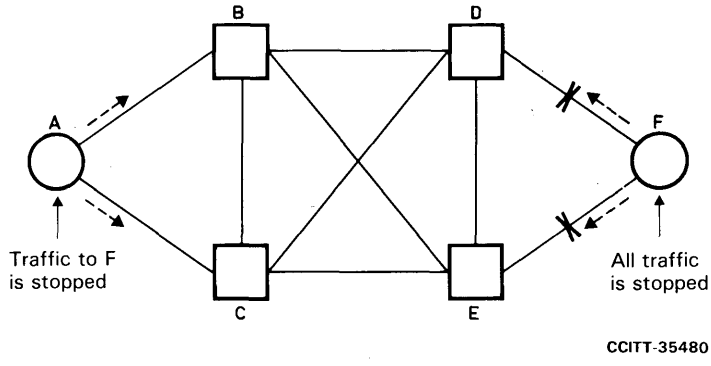



FIGURE A-18/Q.705

**Failure of links DF and EF**

A.4.4.1 *Failure of link DF*

When the failure of link DF is detected, D and F perform the changeover procedure; D diverts traffic, destined to F, to link DE, while F concentrates all the outgoing traffic on link FE.

In addition, D sends to E a transfer-prohibited message, referred to destination F; E will thus start sending of signalling-route-set-test messages, referred to F, towards D (see also § A.4.1.1).

A.4.4.2 *Failure of link EF in the presence of failure of link DF*

a) When the failure of link EF is detected, the following applies:

   i) Since all destinations become inaccessible F stops sending all signalling traffic.

   ii) E sends to B, C and D a transfer-prohibited message, referred to destination F. B, C and D start periodic sending of signalling-route-set-test messages referred to F to E.

b) When D receives the transfer-prohibited message, it sends to B and C a transfer-prohibited message, referred to destination F (see Recommendation Q.704, § 13.2.2 ii)). B and C start periodic sending of test messages referred to F to D.

c) When B receives the transfer-prohibited messages from D and E, it sends a transfer-prohibited message to C; the same applies for C (it sends the message to B). As soon as B and C have received the transfer-prohibited messages from all the three possible routes (BD, BE and BC, or CD, CE and CB respectively), they send a transfer-prohibited message to A.

   *Note* – Depending on the sequence of reception of transfer-prohibited messages at B or C, they may start a forced rerouting procedure on a route not yet declared to be unavailable; such procedure is then aborted as soon as a transfer-prohibited message is received also from that route.

d) As soon as A receives the transfer-prohibited messages from B and C, it declares destination F inaccessible and stops sending traffic towards it. Moreover, it starts the periodic sending of signalling-route-set-test messages, referred to F, to B and C.

A.4.4.3 *Restoration of link EF in the presence of failure on link DF*

a) When restoration of link EF is completed, the following applies:

   i) Signalling point F restarts traffic on link EF.

   ii) E sends a transfer-allowed message, referred to destination F, to B, C and D; moreover it restarts traffic on the restored link.

b) When B and C receive the transfer-allowed message, they send a transfer-allowed message to A and C or A and B, respectively and they stop sending signalling-route-set-test messages to E; moreover, they restart the concerned traffic on link BE or CE respectively.

c) When D receives the transfer-allowed message from E, it sends transfer-allowed messages to B and C and stops sending signalling-route-set-test messages to E; moreover, it starts the concerned traffic on link DE. On receipt of the transfer-allowed message, B and C will divert to links BD and CD, by means of a controlled rerouting procedure, traffic carried by links BE and CE for which they are the normal links (see § A.3.3). Moreover, they will stop sending signalling-route-set-test messages to D.

   *Note* – According to the rules stated in Recommendation Q.704, § 13.3.2, on receipt of transfer-allowed messages from E [phase b) above], B and C should send transfer-allowed messages also to D and E. However, this is not appropriate in the network configurations such as the one here considered, taking into account that:

   – there is no route, for example, from D (or E) to F via B (or C) and therefore the transfer-allowed messages would be ignored by D and E;

   – on restarting traffic to F on links BD, BE, CD and CE it would anyway be necessary that B and C send transfer-prohibited messages to D and E, which would contradict the previous transfer-allowed messages.

d) As soon as A receives a transfer-allowed message from B or C, it restarts signalling traffic to B and C. If traffic has already been restarted on one link when the transfer-allowed message is received on the other link, a changeback procedure is performed to establish the normal routing situation on both links (i.e. to divert part of the traffic on the latter link).

A.4.4.4 *Restoration of link DF*

When the restoration of link DF is completed, the following applies:

a) D initiates the changeback procedure to link DF; moreover, it sends to E a transfer-allowed message, referred to destination F,

b) F sends signalling-route-set-test message to D referred to the destination points it normally accesses via D. It initiates the changeback procedure to link DF; this procedure refers only to the traffic for which link DF is the normal one, according to the routing rules.

A.5 *Explanatory note from the implementors forum for clarification of load sharing*

A.5.1 In general, to improve the distribution of traffic, load sharing at a particular signalling point (amongst link sets to a given destination) will be on the basis of a part of the signalling link selection field which is different than that part used for load sharing amongst signalling links within a selected link set. In the example represented in Figure 5/Q.704, if link set DF contains more than one signalling link, then the least significant bit of the signalling link selection field is not used in sharing traffic within link set DF amongst the signalling links. Similar considerations can apply to link set DE.

A.5.2 At an originating signalling point it is assumed that for a given signalling relation, signalling link selection field values are evenly distributed and traffic is shared over the appropriate link sets and signalling links within each link set on this basis. In general, to achieve this a different oad sharing rule is needed for each number of link sets, and each number of signalling links within a link set, over which traffic is to be shared. The intention is to attain, for a given signalling relation, as een as possible a traffic balance over the link sets and the signalling links within each link set, based on the signalling link selection field and the numbers of link sets and signalling links within each ink set; such an even traffic balance may result if the fixed part of the signalling link selection field is not excluded from consideration by the load sharing rules.

A.5.3 At a signalling transfer point, for a given signalling relation, signalling link selection field values may not be evenly distributed (see Figure 5/Q.704, signalling transfer point E). A different set of load sharing rules to those for originating signalling points may be provided to deal with this possibility. These are again based on the signalling link selection field and the numbers of link sets and signalling links within each link set, but assume that a particular part of the signalling link selection field is fixed. The fixed part of the signalling link selection field may be different at different signalling transfer points. Where signalling messages for different signalling relations arriving at a particular signalling transfer point do not have the same part of the signalling link selection field fixed, an uneven sharing of traffic for a particular signalling relation amongst the relevant link sets and signalling links within each link set may result.

**Recommendation Q.706**

## MESSAGE TRANSFER PART SIGNALLING PERFORMANCE

The message transfer part of Signalling System No. 7 is designed as a joint transport system for the messages of different users. The requirements of the different users have to be met by the Message Transfer Part. These requirements are not necessarily the same and may differ in importance and stringency.

In order to satisfy the individual requirements of each user the Message Transfer Part of Signalling System No. 7 is designed in such a way that it meets the most stringent User Part requirements envisaged at the time of specification. To this end, the requirements of the telephone service, the data transmission service and the signalling network management, in particular, were investigated. It is assumed that a signalling performance which satisfies the requirements mentioned above will also meet those of future users.

In the light of the above, signalling system performance is understood to be the capability of the Message Transfer Part to transfer messages of variable length for different users in a defined manner. In order to achieve a proper signalling performance, three groups of parameters have to be taken into account:

- The first group covers the objectives derived from the requirements of the different users. The aims are limitation of message delay, protection against all kinds of failures and guarantee of availability.
- The second group covers the features of the signalling traffic, such as the loading potential and the structure of the signalling traffic.
- The third group covers the given environmental influences, such as the characteristics (e.g. error rate and proneness to burst) of the transmission media.

The three groups of parameters are considered in the specification of the procedures to enable the Message Transfer Part to transfer the messages in such a way that the signalling requirements of all users are met and that a uniform and satisfactory overall signalling system performance is achieved.

## 1 Basic parameters related to Message Transfer Part signalling performance

Signalling performance is defined by a great number of different parameters. In order to ensure a proper signalling performance for all users to be served by the common Message Transfer Part, the following design objectives are established for the Message Transfer Part.

### 1.1 *Unavailability of a signalling route set*

The unavailability of a signalling route set is determined by the unavailability of the individual components of the signalling network (signalling links and the signalling points) and by the structure of a signalling network.

The unavailability of a signalling route set should not exceed a total of 10 minutes per year.

The unavailability of a signalling route set within a signalling network may be improved by replication of signalling links, signalling paths and signalling routes.

### 1.2 *Unavoidable message transfer part malfunction*

The Message Transfer Part of Signalling System No. 7 is designed to transport messages in a correct sequence. In addition, the messages are protected against transmission errors. However, a protection against transmission errors cannot be absolute. Furthermore, mis-sequencing and loss of messages in the Message Transfer Part cannot be excluded in extreme cases.

For all User Parts, the following conditions are guaranteed by the Message Transfer Part:

a) *Undetected errors*

On a signalling link employing a signalling data link which has the error rate characteristic as described in Recommendation Q.702 not more than one in $10^{10}$ of all signal unit errors will be undetected by the message Transfer Part.

b) *Loss of messages*

Not more than one in $10^{7}$ messages will be lost due to failure in the message transfer part.

c) *Messages out-of-sequence*

Not more than one in $10^{10}$ messages will be delivered out-of-sequence to the User Parts due to failure in the message transfer part. This value also includes duplication of messages.

### 1.3 *Message transfer times*

This parameter includes:

- handling times at the signalling points (see § 4.3);
- queueing delays including retransmission delays (see § 4.2);
- signalling data link propagation times.

### 1.4 *Signalling traffic throughput capability*

Needs further study (see § 2.2).

## 2 Signalling traffic characteristics

### 2.1 *Labelling potential*

The design of Signalling System No. 7 provides the potential for labels to identify 16 384 signalling points. For each of the 16 different User Parts a number of user transactions may be identified, e.g. in the case of the telephone service up to 4096 speech circuits.

### 2.2 *Loading potential*

Considering that the load per signalling channel will vary according to the traffic characteristics of the service, to the user transactions served and to the number of signals in use, it is not practicable to specify a general maximum limit of user transactions that a signalling channel can handle. The maximum number of user transactions to be served must be determined for each situation, taking into account the traffic characteristics applied so that the total signalling load is held to a level which is acceptable from different points of view.

When determining the normal load of the signalling channel, account must be taken of the need to ensure a sufficient margin for peak traffic loads.

The loading of a signalling channel is restricted by several factors which are itemized below.

#### 2.2.1 *Queueing delay*

The queueing delay in absence of disturbances is considerably influenced by the distribution of the message length and the signalling traffic load (see § 4.2).

#### 2.2.2 *Security requirements*

The most important security arrangement is redundancy in conjunction with changeover. As load sharing is applied in normal operation, the load on the individual signalling channels has to be restricted so that, in the case of changeover, the queueing delays do not exceed a reasonable limit. This requirement has to be met not only in the case of changeover to one predetermined link but also in the case of load distribution to the remaining links.

#### 2.2.3 *Capacity of sequence numbering*

The use of 7 bits for sequence numbering finally limits the number of signal units sent but not yet acknowledged to the value of 127.

In practice this will not impose a limitation on the loading potential.

#### 2.2.4 *Signalling channels using lower bit rates*

A loading value for a signalling channel using bit rates of less than 64 kbit/s will result in greater queueing delays than the same loading value for a 64-kbit/s signalling channel.

### 2.3 *Structure of signalling traffic*

The Message Transfer Part of Signalling System No. 7 serves different User Parts as a joint transport system for messages. As a result, the structure of the signalling traffic largely depends on the types of User Parts served. It can be assumed that at least in the near future the telephone service will represent the main part of the signalling traffic also in integrated networks.

It cannot be foreseen yet how the signalling traffic is influenced by the integration of existing and future services. The traffic models given in § 4.2.4 have been introduced in order to consider as far as possible the characteristics and features of different services within an integrated network. If new or more stringent requirements are imposed on signalling (e.g. shorter delays) as a consequence of future services, they should be met by appropriate dimensioning of the load or by improving the structure of the signalling network.

## 3 Parameters related to transmission characteristics

No special transmission requirements are envisaged for the signalling links of Signalling System No. 7. Therefore, System No. 7 provides appropriate means in order to cope with the given transmission characteristics of ordinary links. The following items indicate the actual characteristics to be expected – as determined by the responsible Study Groups – and their consequences on the specifications of the Signalling System No. 7 Message Transfer Part.

### 3.1 *Application of Signalling System No. 7 to 64-kbit/s links*

The Message Transfer Part is designed to operate satisfactorily with the following transmission characteristics:

a) a long-term bit error rate of the signalling data link of less than $10^{-6}$ [1];

b) a medium-term bit error rate of less than $10^{-4}$;

c) random errors and error bursts including long bursts which might occur in the digital link due to, for instance, loss of frame alignment or octet slips in the digital link. The maximum tolerable interruption period is specified for the signal unit error rate monitor (see Recommendation Q.703, § 10.2).

### 3.2 *Application of Signalling System No. 7 to links using lower bit rates*

(Needs further study.)

## 4 Parameters of influence on signalling performance

### 4.1 *Signalling network*

Signalling System No. 7 is designed for both associated and nonassociated applications. The reference section in such applications is the signalling route set, irrespective of whether it is served in the associated or quasi-associated mode of operation.

For every signalling route set in a signalling network, the unavailability limit indicated in § 1.1 has to be observed irrespective of the number of signalling links in tandem of which it is composed.

#### 4.1.1 *International signalling network*

(Needs further study.)

#### 4.1.2 *National signalling network*

(Needs further study.)

### 4.2 *Queueing delays*

The Message Transfer Part handles messages from different User Parts on a time-shared basis. With time-sharing, signalling delay occurs when it is necessary to process more than one message in a given interval of time. When this occurs, a queue is built up from which messages are transmitted in order of their times of arrival.

There are two different types of queueing delays: queueing delay in the absence of disturbances and total queueing delay.

#### 4.2.1 *Assumptions for derivation of the formulas*

The queueing delay formulas are basically derived from the $M/G/1$ queue with priority assignment. The assumptions for the derivation of the formulas in the absence of disturbances are as follows:

a) the interarrival time distribution is exponential ($M$);

b) the service time distribution is general ($G$);

c) the number of server is one (1);

d) the service priority refers to the transmission priority within level 2 (see Recommendation Q.703, § 11.2); however, the link status signal unit and the independent flag are not considered;

e) the signalling link loop propagation time is constant including the process time in signalling terminals; and

f) the forced retransmission case of the preventive cyclic retransmission method is not considered.

In addition, for the formulas in the presence of disturbances, the assumptions are as follows:

g) the transmission error of the message signal unit is random;

h) the errors are statistically independent of each other;

i) the additional delay caused by the retransmission of the erroneous signal unit is considered as a part of the waiting time of the concerned signal unit; and

j) in case of the preventive cyclic retransmission method, after the error occurs, the retransmitted signal units of second priority are accepted at the receiving end until the sequence number of the last sent new signal unit is caught up by that of the last retransmitted signal unit.

Furthermore, the formula of the proportion of messages delayed more than a given time is derived from the assumption that the probability density function of the queueing delay distribution may be exponentially decreasing where the delay time is relatively large.

4.2.2 *Factors and parameters*

a) The notations and factors required for calculation of the queueing delays are as follows:

$Q_a$ mean queueing delay in the absence of disturbances

$\sigma_a^2$ variance of queueing delay in the absence of disturbances

$Q_t$ mean total queueing delay

$\sigma_t^2$ variance of total queueing delay

$P(T)$ proportion of messages delayed more than $T$

$a$ traffic loading by message signal units (MSU) (excluding retransmission)

$T_m$ mean emission time of message signal units

$T_f$ emission time of fill-in signal units

$T_L$ signalling loop propagation time including processing time in signalling terminal

$P_u$ error probability of message signal units

$$k_1 = \frac{\text{2nd moment of message signal units emission time}}{T_m^2}$$

$$k_2 = \frac{\text{3rd moment of message signal units emission time}}{T_m^3}$$

$$k_3 = \frac{\text{4th moment of message signal units emission time}}{T_m^4}$$

*Note* – As a consequence of zero insertion at level 2 (see Recommendation Q.703, § 3.2), the length of the emitted signal unit will be increased by approximately 1.6 percent on average. However, this increase has negligible effect on the calculation.

b) The parameters used in the formulas are as follows:

$$t_f = T_f / T_m$$

$$t_L = T_L / T_m$$

for the basic method,

$$E_1 = 1 + P_u t_L$$

$$E_2 = k_1 + P_u t_L (t_L + 2)$$

$$E_3 = k_2 + P_u t_L (t_L^2 + 3t_L + 3k_1)$$

for the preventive cyclic retransmission (PCR) method,

$a_3 = \exp(-at_L)$: traffic loading caused by fill-in signal units.

$$a_z = 1 - a - a_3$$

$$H_1 = at_L$$

$$H_2 = at_L(k_1 + at_L)$$

$$H_3 = at_L(k_2 + 3at_Lk_1 + a^2t_L^2)$$

$$F_1 = at_L/2$$

$$F_2 = at_L(k_1/2 + at_L/3)$$

$$F_3 = at_L(k_2/2 + at_Lk_1 + a^2t_L^2/4)$$

$$q_a = \frac{k_1(a + a_z) + a_3t_f}{2(1 - a)}$$

$$s_a = \frac{ak_1}{1 - a} q_a + \frac{k_2(a + a_z) + a_3t_f^2}{3(1 - a)}$$

$$t_a = \frac{3ak_1s_a + 2ak_2q_a}{2(1 - a)} + \frac{(a + a_z)k_3 + a_3t_f^3}{4(1 - a)}$$

$$Z_1 = 2 + P_u(1 + H_1)$$

$$Z_2 = 4K_1 + P_u(5k_1 + 3H_1 + H_2)$$

$$Z_3 = 8k_2 + P_u(19k_2 + 27k_1H_1 + 9H_2 + H_3)$$

$$Y_2 = s_a + 4k_1 + F_2 + 2\{q_a(2 + F_1) + 2F_1\}$$

$$Y_3 = t_a + 8k_2 + F_3 + 3\{s_a(2 + F_1) + q_a(4k_1 + F_2) + 2F + 2 + 4k_1F_1\} + 12q_aF_1$$

$$\alpha = \frac{1 - a\{2 + P_u(1 + at_L)\}}{2 + q_a + at_L/2}$$

$$q_d = \frac{aZ_2 + \alpha Y_2}{2(1 - aZ_1)}$$

$$s_d = \frac{aZ_2}{1 - aZ_1} q_d + \frac{aZ_3 + \alpha Y_3}{3(1 - aZ_1)}$$

$$q_b = \frac{q_a + 1 + F_1}{1 - a}$$

$$s_b = \frac{s_a + k_1 + F_2}{(1 - a)^3} + \frac{2\{q_a(1 + F_1) + F_1\}}{(1 - a)^2}$$

$$q_c = \frac{q_d + 1 + P_u(1 + H_1)}{1 - a}$$

$$s_c = \frac{s_d + k_1 + P_u(3k_1 + H_2)}{(1 - a)^3} + 2\frac{q_d + P_u\{q_d(1 + H_1) + 2H_1\}}{(1 - a)^2}$$

$$P_V = P_ua \frac{q_a + 2 + at_L/2}{1 - 2a} \left(1 + P_u \frac{a + a^2t_L}{1 - 2a}\right)$$

4.2.3 *Formulas*

The formulas of the mean and the variance of the queueing delays are described in Table 1/Q.706. The proportion of messages delayed more than a given time $T_x$ is:

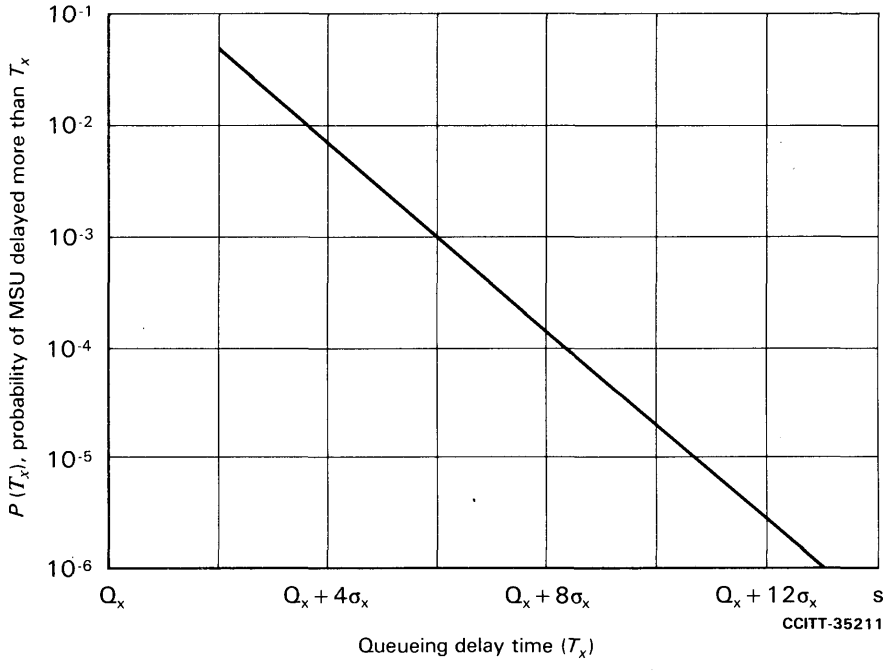
$$P(T_x) \simeq \exp\left(-\frac{T_x - Q_x + \sigma_x}{\sigma_x}\right)$$

where $Q_x$ and $\sigma_x$ denote the mean and the standard deviation of queueing delay, respectively. This approximation is better suited in absence of disturbances. In the presence of disturbances the actual distribution may be deviated further. Relation between $P(T_x)$ and $T_x$ is shown in Figure 1/Q.706.

4.2.4 *Examples*

Assuming the traffic models given in Table 2/Q.706, examples of queueing delays are calculated as listed in Table 3/Q.706.

*Note* – The values in the table were determined based on TUP messages. With the increase of the effective message length, using ISUP and TC, these values may be expected to be increased during the course of further study.




$Q_x$ Mean queueing delay (see Figure 2/Q.706)
$\sigma_x$ Standard deviation (see Figure 3/Q.706)

FIGURE 1/Q.706

**Probability of message signal unit delayed more than $T_x$**

TABLE 1/Q.706

**Queueing delay formula**

| Error correction method | Disturbance | Mean $Q$ | Variance $\sigma^2$ |
|---|---|---|---|
| Basic | Absence | $\frac{Q_a}{T_m} = \frac{t_f}{2} + \frac{ak_1}{2(1-a)}$ | $\frac{\sigma_a^2}{T_m^2} = \frac{t_f^2}{12} + \frac{a[4k_2 - (4k_2 - 3k_1^2)a]}{12(1-a)^2}$ |
| | Presence | $\frac{Q_t}{T_m} = \frac{t_f}{2} + \frac{aE_2}{2(1-aE_1)} + E_1 - 1$ | $\frac{\sigma_t^2}{T_m^2} = \frac{t_f^2}{12} + \frac{a[4E_3 - (4E_1E_3 - 3E_2^2)a]}{12(1-aE_1)^2} + P_u(1-P_u)t_L^2$ |
| Preventive cyclic retransmission | Absence | $\frac{Q_a}{T_m} = q_a$ | $\frac{\sigma_t^2}{T_m^2} = s_a - q_a^2$ |
| | Presence | $\frac{Q_t}{T_m} = (1 - P_u - P_v)\, q_a + P_u q_b + P_v q_c$ | $\frac{\sigma_t^2}{T_m^2} = (1 - P_u - P_v)\, s_a + P_u s_b + P_v s_c - \frac{Q_t^2}{T_m^2}$ |

TABLE 2/Q.706

**Traffic model**

| Model | A | B | |
|---|---|---|---|
| Message length (bits) | 120 | 104 | 304 |
| Percent | 100 | 92 | 8 |
| Mean message length (bits) | 120 | 120 | |
| $k_1$ | 1.0 | 1.2 | |
| $k_2$ | 1.0 | 1.9 | |
| $k_3$ | 1.0 | 3.8 | |

TABLE 3/Q.706

**List of examples**

| Figure | Error control | Queueing delay | Disturbance | Model |
|---|---|---|---|---|
| 2/Q.706 | Basic/PCR | Mean | Absence | A and B |
| 3/Q.706 | Basic/PCR | Standard deviation | Absence | A and B |
| 4/Q.706 | Basic | Mean | Presence | A |
| 5/Q.706 | Basic | Standard deviation | Presence | A |
| 6/Q.706 | PCR | Mean | Presence | A |
| 7/Q.706 | PCR | Standard deviation | Presence | A |

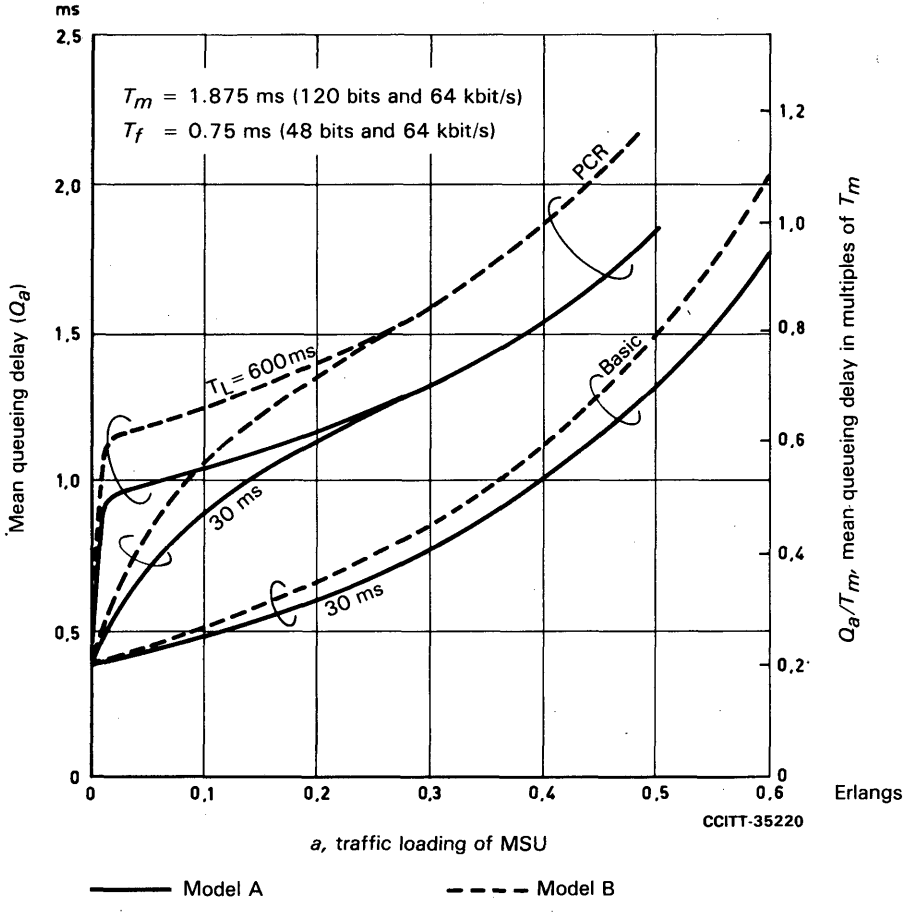



FIGURE 2/Q.706

**Mean queueing delay of each channel of traffic in absence of disturbance**

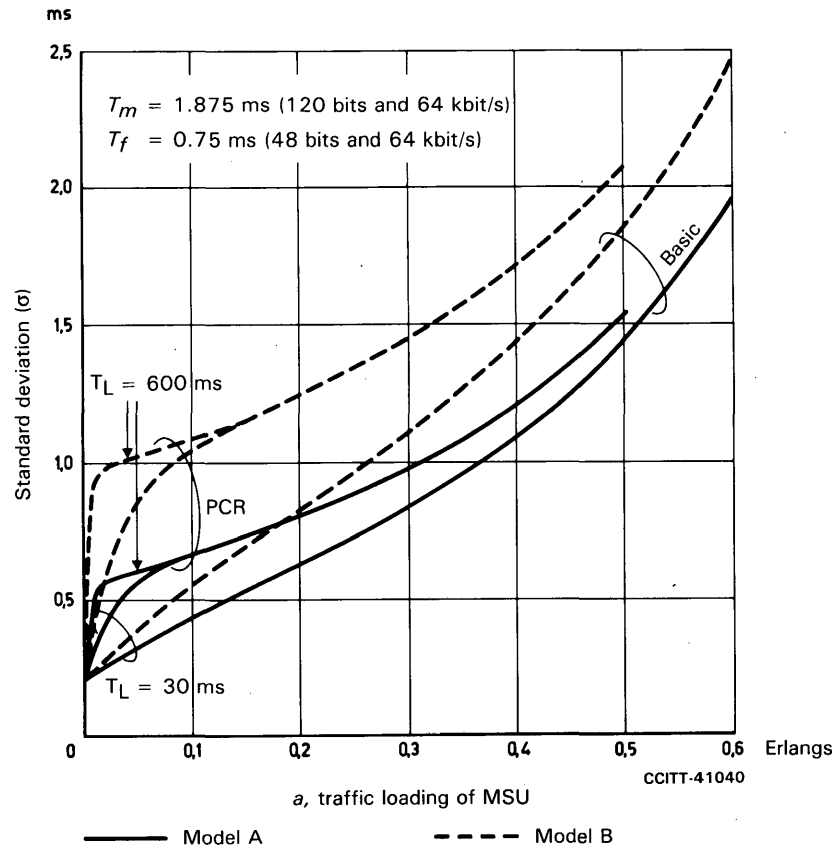



FIGURE 3/Q.706

**Standard deviation of queueing delay of each channel of traffic in absence of disturbance**

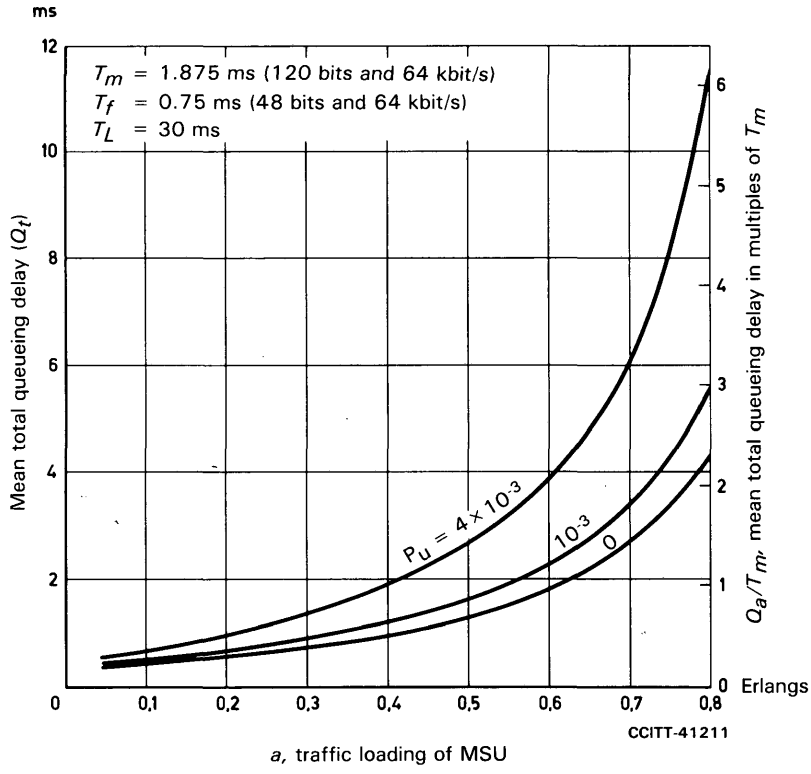
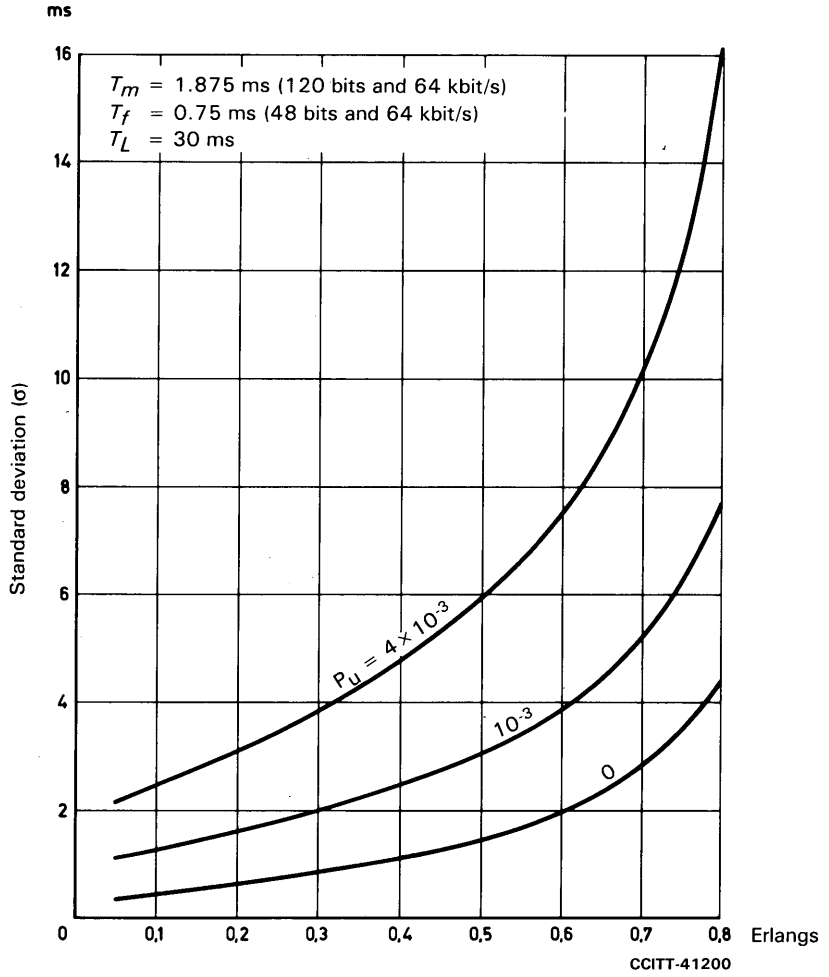



FIGURE 4/Q.706

**Mean total queueing delay of each channel of traffic; basic error correction method**




*a,* traffic loading of MSU

FIGURE 5/Q.706

**Standard deviation of queueing delay of each channel of traffic; basic error correction method**

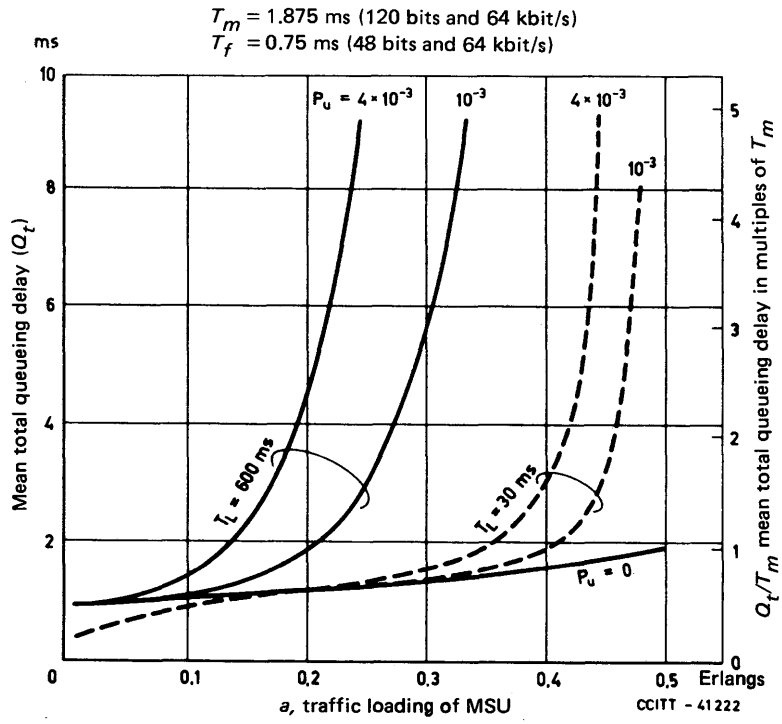



FIGURE 6/Q.706

**Mean total queueing delay of each channel of traffic: preventive cyclic retransmission error correction method**

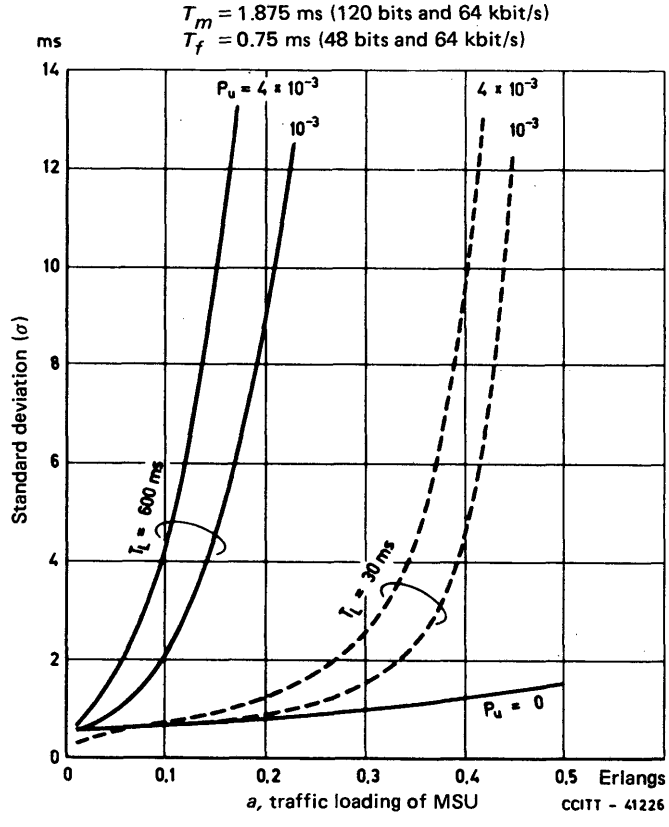



FIGURE 7/Q.706

**Standard deviation of queueing delay of each channel of traffic: preventive cyclic retransmission error correction method**

4.3 *Message transfer times*

Within a signalling relation, the Message Transfer Part transports messages from the originating User Part to the User Part of destination, using several signalling paths. The overall message transfer time needed depends on the message transfer time components (a) to (e) involved in each signalling path.

4.3.1 *Message transfer time components and functional reference points*

A signalling path may include the following functional signalling network components and transfer time components.

a) Message Transfer Part sending function at the point of origin (see Figure 8/Q.706).

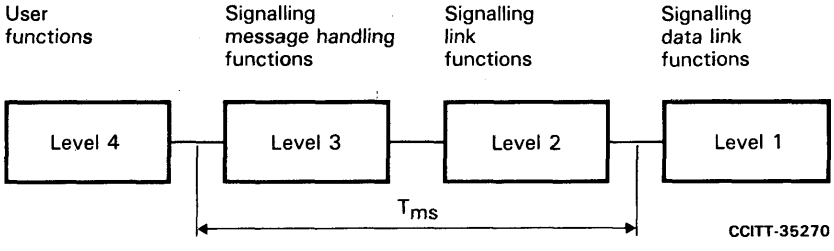
b) Signalling transfer point function (see Figure 9/Q.706).

c) Message Transfer Part receiving function at the point of destination (see Figure 10/Q.706).

d) Signalling data link propagation time (see Figure 11/Q.706).

e) Queueing delay.

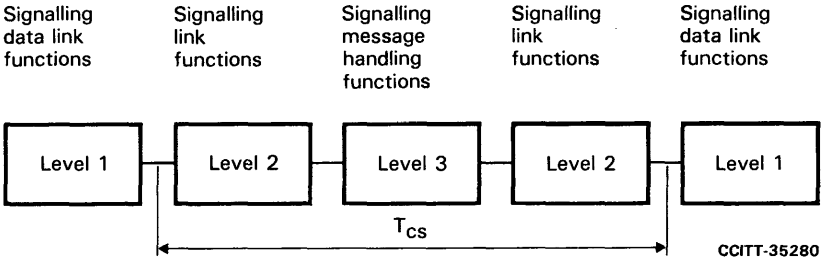
An additional increase of the overall message transfer times is caused by the queueing delays. These are described in § 4.2.




$T_{ms}$ Message Transfer Part sending time

FIGURE 8/Q.706

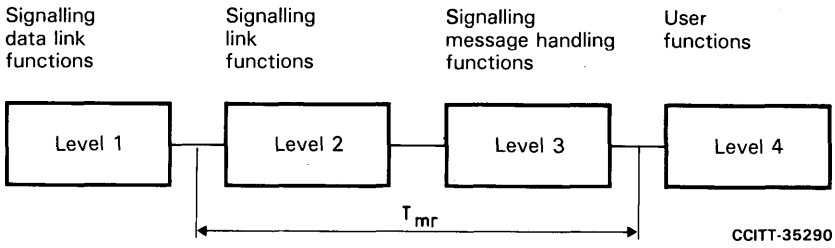
**Functional diagram of the Message Transfer Part sending time**




$T_{cs}$ Message transfer time at signalling transfer points

FIGURE 9/Q.706

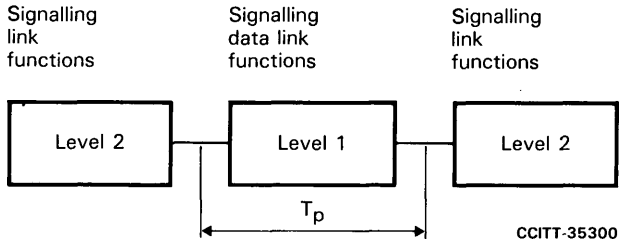
**Functional diagram of the message transfer time at signalling transfer points**




$T_{mr}$ Message Transfer Part receiving time

FIGURE 10/Q.706

**Functional diagram of the Message Transfer Part receiving time**




$T_p$ Propagation time of the data channel

FIGURE 11/Q.706

**Functional diagram for the propagation time**

4.3.2 *Definitions*

4.3.2.1 **message transfer part sending time $T_{ms}$**

*F: temps d'émission du Sous-système Transport de Messages $T_{ms}$*

*S: tiempo de emisión de la parte de transferencia de mensajes $T_{ms}$*

$T_{ms}$ is the period which starts when the last bit of the message has left the User Part and ends when the last bit of the signal unit enters the signalling data link for the first time. It includes the queueing delay in the absence of disturbances, the transfer time from level 4 to level 3, the handling time at level 3, the transfer time from level 3 to level 2, and the handling time in level 2.

4.3.2.2 **message transfer time at signalling transfer points $T_{cs}$**

*F: temps de transfert des messages aux points de transfert sémaphore $T_{cs}$*

*S: tiempo de transferencia de mensajes en los puntos de transferencia de la señalización $T_{cs}$*

$T_{cs}$ is the period, which starts when the last bit of the signal unit leaves the incoming signalling data link and ends when the last bit of the signal unit enters the outgoing signalling data link for the first time. It also includes the queueing delay in the absence of disturbances but not the additional queueing delay caused by retransmission.

4.3.2.3 **message transfer part receiving time $T_{mr}$**

*F: temps de réception du Sous-système Transport de Messages $T_{mr}$*

*S: tiempo de recepción de la parte de transferencia de mensajes $T_{mr}$*

$T_{mr}$ is the period which starts when the last bit of the signal unit leaves the signalling data link and ends when the last bit of the message has entered the User Part. It includes the handling time in level 2, the transfer time from level 2 to level 3, the handling time in level 3 and the transfer time from level 3 to level 4.

4.3.2.4 **data channel propagation time $T_p$**

*F: temps de propagation sur la voie de données $T_p$*

*S: tiempo de propagación del canal de datos $T_p$*

$T_p$ is the period which starts when the last bit of the signal unit has entered the data channel at the sending side and ends when the last bit of the signal unit leaves the data channel at the receiving end irrespective of whether the signal unit is disturbed or not.

4.3.3 *Overall message transfer times*

The overall message transfer time $T_o$ is referred to the signalling relation. $T_o$ starts when the message has left the user part (level 4) at the point of origin and ends when the message has entered the user part (level 4) at the point of destination.

The definition of the overall message transfer time and the definitions of the individual message transfer time components give rise to the following relationships:

a) In the absence of disturbances

$$T_{oa} = T_{ms} + \sum_{i=1}^{n+1} T_{pi} + \sum_{i=1}^{n} T_{csi} + T_{mr}$$

b) In the presence of disturbances

$$T_o = T_{oa} + \Sigma (Q_t - Q_a)$$

Here

$T_{oa}$ overall message transfer time in the absence of disturbances

$T_{ms}$ Message Transfer Part sending time

$T_{mr}$ Message Transfer Part receiving time

$T_{cs}$ Message transfer time at signalling transfer points

$n$ number of STPs involved

$T_p$ data channel propagation time

$T_o$ overall message transfer time in the presence of disturbances

$Q_t$ total queueing delay (see § 4.2)

$Q_a$ queueing delay in the absence of disturbances (see § 4.2)

*Note* – For $\Sigma(Q_t - Q_a)$, all signalling points in the signalling relation must be taken into account.

4.3.4 *Estimates for message transfer times*

(Needs further study.)

The estimates must take account of:

- the length of the signal unit,
- the signalling traffic load,
- the signalling bit rate.

The estimates for $T_{mr}$, $T_{ms}$ and $T_{cs}$ will be presented in the form of:

- mean values,
- 95% level values.

The estimates for $T_{cs}$ for a signalling transfer point are given in Table 4/Q.706.

TABLE 4/Q.706

| STP signalling traffic load | Message transfer time at an STP ($T_{cs}$) in ms | |
|---|---|---|
| | Mean | 95 % |
| Normal | 20 | 40 |
| +15 % | 40 | 80 |
| +30 % | 100 | 200 |

*Note* – the values in the table were determined based on TUP messages. With the increase of the effective message length, using ISUP and TC, these values may be expected to be increased during the course of further study.

These figures are related to 64-kbit/s signalling bit rate. The normal signalling traffic load is that load for which the signalling transfer point is engineered. A mean value of 0.2 Erlang per signalling link is assumed. The message length distribution is as given in Table 2/Q.706.

### 4.4 *Error control*

During transmission, the signal units are subject to disturbances which lead to a falsification of the signalling information. The error control reduces the effects of these disturbances to an acceptable value.

Error control is based on error detection by redundant coding and on error correction by retransmission. Redundant coding is performed by generation of 16 check bits per signal unit based on the polynomial described in Recommendation Q.703, § 4.2. Moreover, the error control does not introduce loss, duplication or mis-sequencing of messages on an individual signalling link.

However, abnormal situations may occur in a signalling relation, which are caused by failures, so that the error control for the signalling link involved cannot ensure the correct message sequence.

### 4.5 *Security arrangements*

The security arrangements have an essential influence on the observance of the availability requirements listed in § 1.1 for a signalling relation.

In the case of Signalling System No. 7, the security arrangements are mainly formed by redundancy in conjunction with changeover.

#### 4.5.1 *Types of security arrangements*

In general, a distinction has to be made between security arrangements for the individual components of the signalling network and security arrangements for the signalling relation. Within a signalling network, any security arrangement may be used, but it must be ensured that the availability requirements are met.

4.5.1.1 *Security arrangements for the components of the signalling network*

Network components, which form a signalling path when being interconnected, either have constructional security arrangements which exist from the very beginning (e.g. replication of the controls at the exchanges and signalling transfer points) or can be replicated, if need be (e.g. signalling data links). For security reasons, however, replication of signalling data links is effected only if the replicated links are independent of one another (e.g. multipath routing). In the case of availability calculations for a signalling path set, special care has to be taken that the individual signalling links are independent of one another.

4.5.1.2 *Security arrangements for signalling relations*

In quasi-associated signalling networks where several signalling links in tandem serve one signalling relation, the security arrangements for the network components, as a rule, do not ensure sufficient availability of the signalling relation. Appropriate security arrangements must therefore be made for the signalling relations by the provision of redundant signalling path sets, which have likewise to be independent of one another.

4.5.2 *Security requirements*

In the case of 64-kbit/s signalling links, a signalling network has to be provided with sufficient redundancy so that the quality of the signalling traffic handled is still satisfactory. (Application of the above to signalling links using lower bit rates needs further study.)

4.5.3 *Time to initiate changeover*

If individual signalling data links fail, due to excessive error rates, changeover is initiated by signal unit error monitoring (see Recommendation Q.703, § 8). With signal unit error monitoring, the time between the occurrence of the failure and the initiation of changeover is dependent on the message error rate (a complete interruption will result in an error rate equal to 1).

Changeover leads to substantial additional queueing delays. To keep the latter as short as possible, the signalling traffic affected by an outage is reduced to a minimum by the use of load sharing on all existing signalling links.

4.5.4 *Changeover performance times*

There are two performance times associated with link changeover. Both times are maximum time values (not normal values). They are defined to be the point at which 95% of the events occur within the recommended performance time at a signalling point traffic load that is 30% above normal.

The performance times are measured from outside the signalling point.

4.5.4.1 *Failure response time*

This time describes the time taken by a signalling point to recognize that a changeover is needed for a signalling link. This time begins when the signalling link is unavailable, and ends when the signalling point sends a changeover (or emergency changeover) order to the remote signalling point. A link is unavailable when a signalling unit with status indication out of service (SIOS) or processor outage (SIPO) is sent or received on the link.

Failure response time (maximum permissible): 500 ms.

4.5.4.2 *Answer time to changeover order*

This time describes the time taken by a signalling point to answer a changeover (or emergency changeover) order. This time begins when the signalling point receives a changeover (or emergency changeover) order message, and ends when the signalling point sends a changeover (or emergency changeover) acknowledgement message.

Answer time to changeover order (maximum permissible): 300 ms.

4.6 *Failures*

4.6.1 *Link failures*

During transmission, the messages may be subject to disturbances. A measure of the quality of the signalling data link is its signal unit error rate.

Signal unit error monitoring initiates the changeover at a signal unit error rate of about $4 \cdot 10^{-3}$.

The error rate, which Signalling System No. 7 has to cope with, represents a parameter of decisive influence on its efficiency.

As a result of error correction by retransmission, a high error rate causes frequent retransmission of the message signal units and thus long queueing delays.

4.6.2 *Failures in signalling points*

(Needs further study.)

4.7 *Priorities*

Priorities resulting from the meaning of the individual signals are not envisaged. Basically, the principle "first-in – first-out" applies.

Although the service indicator offers the possibility of determining different priorities on a user basis, such user priorities are not yet foreseen.

Transmission priorities are determined by Message Transfer Part functions. They are solely dependent on the present state of the Message Transfer Part and completely independent of the meaning of the signals (see Recommendation Q.703, § 11).

## 5 Performance under adverse conditions

5.1 *Adverse conditions*

(Needs further study.)

5.2 *Influence of adverse conditions*

(Needs further study.)

**Reference**

[1] CCITT Recommendation *Error performance on an international digital connection forming part of an integrated services digital network*, Vol. III, Rec. G.821.

# Recommendation Q.707

## TESTING AND MAINTENANCE

## 1 General

In order to realize the performance requirements described in Recommendation Q.706, means and procedures for signalling network testing and maintenance are required in addition to the means defined in Recommendations Q.703 and Q.704.

## 2 Testing

2.1 *Signalling data link test*

As defined in Recommendation Q.702, § 1, the signalling data link is a bidirectional transmission path for signalling. Testing and maintenance functions can be initiated independently at either end.

The signalling data link and the constituent parts of the digital and analogue versions are described in Recommendation Q.702, § 1.

They must be tested before being put into service to ensure that they meet the requirements of Recommendation Q.702, § 3.

Since interruptions of the signalling data link will affect many transactions, they must be treated with the utmost care. Appropriate special measures should be taken to prevent unauthorized maintenance access which could result in interruptions to service. These special measures may include marking or flagging the equipment and indications on distribution frames or test bays where access is possible (see Recommendation M.1050 [1]).

The signal unit error rate monitor and the alignment error rate monitor described in Recommendation Q.703, § 10, also provide means for detecting deterioration of a signalling data link.

Further studies are required with reference to Recommendation V.51 [2].

### 2.2 *Signalling link test*

As defined in Recommendation Q.703, § 1.1.1 and illustrated in Figure 1/Q.701, the signalling link comprises a signalling data link with signalling link functions at either end.

In the following, an on-line signalling link test procedure is specified which involves communication between the two ends of the concerned signalling link. This procedure is to be used when a signalling link is activated or restored (see Recommendation Q.704, § 12). The signalling link becomes available only if the test is successful. This procedure is intended for use while the signalling link is in service. In addition, local failure detection procedures should be performed at either end; these are not specified in this Recommendation.

In case the signalling link test (SLT) is applied while the signalling link is in service the signalling link test message is sent at regular intervals T2 (see § 5.5). The testing of a signalling link is performed independently from each end.

The ability to send a signalling test acknowledgement message, defined below, must always be provided at a signalling point.

The signalling point initiating the tests transmits a signalling link test message on the signalling link to be tested. This message includes a test pattern which is chosen at the discretion of the end initiating the test. After receiving a signalling link test message, a signalling point responds with a signalling link test acknowledgement message on the signalling link identified by the SLS contained in the signalling link test message. The test pattern included in the signalling link test acknowledgement message is identical to the test pattern received.

The signalling link test will be considered successful only if the received signalling link test acknowledgement message fulfills the following criteria:

a) the SLC identifies the physical signalling link on which the SLTA was received.

b) the OPC identifies the signalling point at the other end of the link.

c) the test pattern is correct.

In the case when the criteria given above are not met or a signalling link test acknowledgement message is not received on the link being tested within T1 (see § 5.5) after the signalling link test message has been sent, the test is considered to have failed and is repeated once. In the case when also the repeated test fails, the following actions have to be taken:

- SLT applied on activation/restoration, the link is put out of service, restoration is attempted and a management system must be informed.
- SLT applied periodically, for further study.

The formats and codes of signalling link test and signalling link test acknowledgement messages used for signalling link testing are specified in § 5.4.

## 3 Fault location

Fault location operations, employing particular manual or automatic internal test equipment are left to the discretion of the individual signalling points.

Tests requiring provision of messages are for further study. See [3].

## 4 Signalling network monitoring

In order to obtain information on the status of the signalling network, monitoring of the signalling activity must be provided (for example measures of the signalling load on the signalling data link). The specification of such means and procedures is contained in Recommendations Q.791 and Q.795.

## 5 Formats and codes of signalling network testing and maintenance messages

### 5.1 *General*

The signalling network testing and maintenance messages are carried on the signalling channel in message signal units, the format of which is described in Recommendation Q.703, § 2. As indicated in Recommendation Q.704, § 14.2.1, these messages are distinguished by the configuration 0001 of the service indicator (SI). The Sub Service Field (SSF) of signalling network testing and maintenance messages is used in accordance with Recommendation Q.704, § 14.2.2.

The Signalling Information Field (SIF) consists of an integral number of octets and contains the label, the heading code and one or more signals and indications.

### 5.2 *Label*

For signalling network testing and maintenance messages, the label has the same structure as the label of signalling network management messages (see Recommendation Q.704, § 15.2).

### 5.3 *Heading code H0*

The heading code H0 is the 4-bit field following the label and identifies the message group. The different heading codes are allocated as follows:

0000 Spare

0001 Test messages

The remaining codes are spare.

### 5.4 *Signalling link test messages*

The format of the signalling link test messages is shown in Figure 1/Q.707.

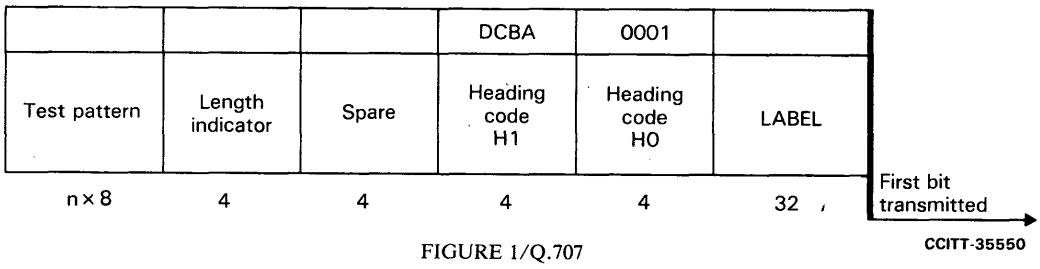



FIGURE 1/Q.707

The signalling link test messages, are made up of the following fields:

- Label: (32 bits), see § 5.2
- Heading code H0: (4 bits)
- Heading code H1: (4 bits)
- Spare bits: (4 bits)
- Length indicator: (4 bits)
- Test pattern: ($n \times 8$ bits, $1 \leqslant n \leqslant 15$).

In the label, the signalling link code identifies the signalling link on which the test message is sent.

The heading code H1 contains signal codes as follows:

bits D C B A
0 0 0 1 signalling link test message (SLTM)
0 0 1 0 signalling link test acknowledgement message (SLTA)

The length indicator gives the number of octets which the test pattern comprises.

The test pattern is an integral number of octets and is chosen at the discretion of the originating point.

### 5.5 *Time-out values and tolerances*

| Q.707 Timer | Range |
|---|---|
| T1 (see § 2.2)<br>Supervision timer for signalling link test acknowledgement message | 4-12 s<br>(equal or greater than T6 of Q.703) |
| T2 (see § 2.2)<br>Interval timer for sending signalling link test messages | 30-90 s |

## 6 State transition diagrams

The state transition diagram is intended to show precisely the behaviour of the signalling system under normal and abnormal conditions as viewed from a remote location. It must be emphasized that the functional partitioning shown in the following diagram is used only to facilitate understanding of the system behaviour and is not intended to specify the functional partitioning to be adopted in a practical implementation of the signalling system.

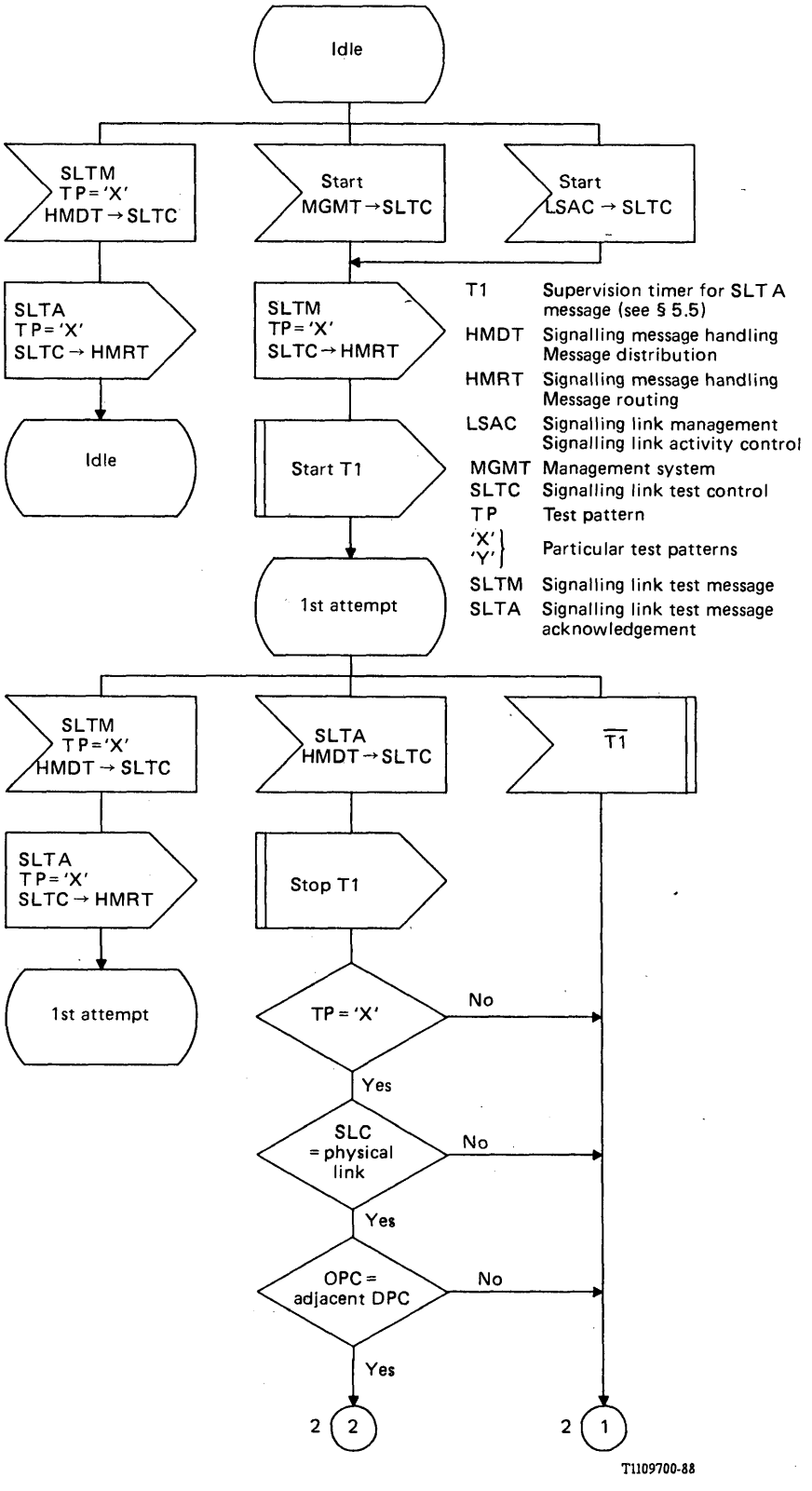



FIGURE 2/Q.707 (Sheet 1 of 2)

**Signalling link test control (SLTC)**

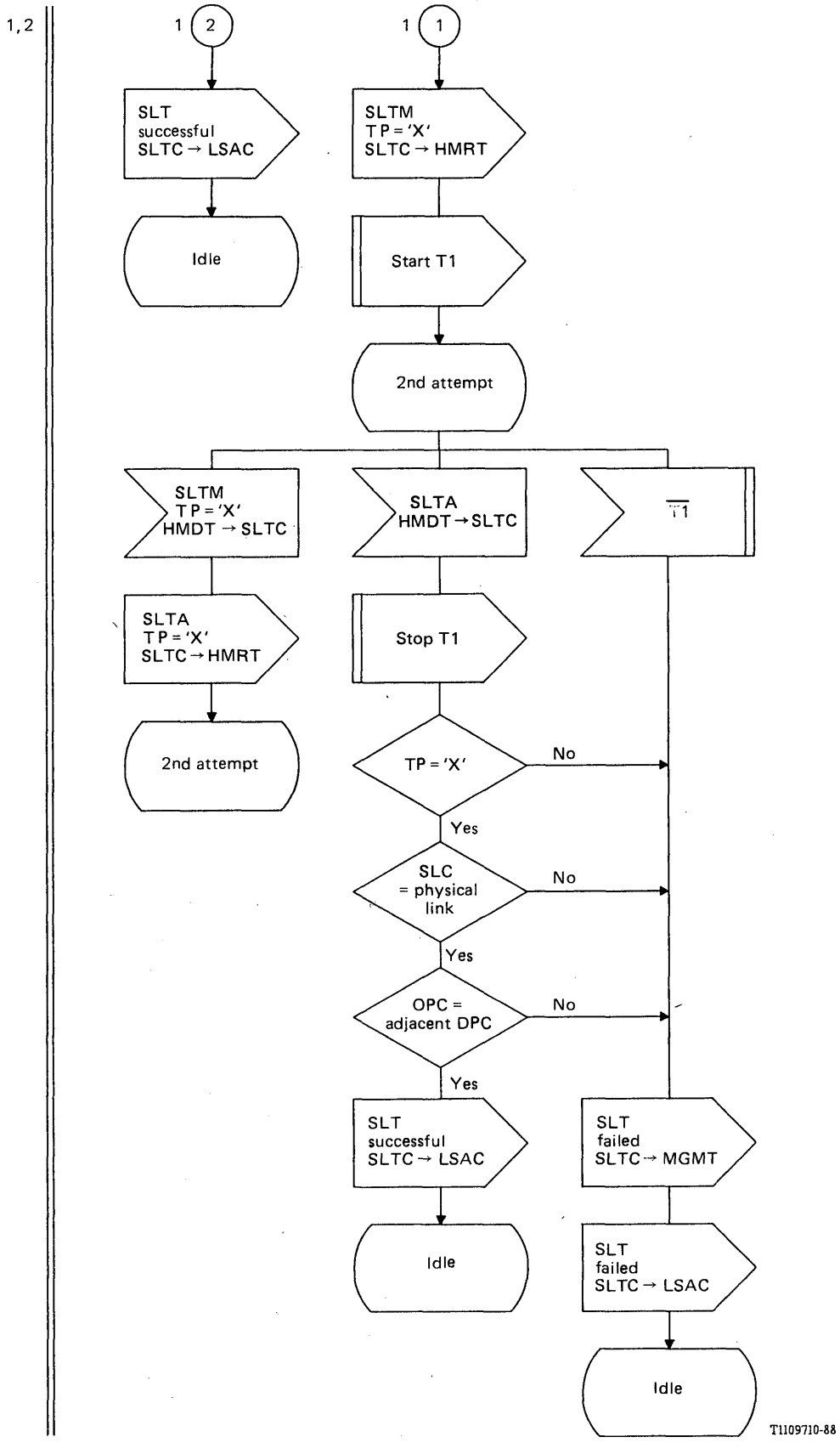



FIGURE 2/Q.707 (Sheet 2 of 2)

**Signalling link test control (SLTC)**

**References**

[1] CCITT Recommendation *Lining up an international point-to-point leased circuit*, Vol. IV, Rec. M.1050.

[2] CCITT Recommendation *Organization of the maintenance of international telephone-type circuits used for data transmission*, Vol. VIII, Rec. V.51.

[3] *Ibid.*, § 5.

**Recommendation Q.708**

## NUMBERING OF INTERNATIONAL SIGNALLING POINT CODES

### 1 Introduction

This Recommendation describes the numbering scheme of international signalling point codes for Signalling System No. 7 networks. The technical aspects of the signalling networks are specified in Recommendation Q.705.

The worldwide signalling network is structured into two functionally independent levels, namely the international and national levels. This structure makes possible a clear division of responsibility for signalling network management and allows numbering plans of signalling points of the international network and the different national networks to be independent of one another.

It is also noted that the point code is intended to be processed within the Message Transfer Part of each signalling point or signalling transfer point, so that there is no direct relationship to the telephone, data, or ISDN numbering.

### 2 Numbering of International Signalling Points

2.1 A 14-bit binary code is used for the identification of signalling points.

2.2 An international signalling point code (ISPC) should be assigned to each signalling point which belongs to the international signalling network. For some network environment, one physical network node may serve as more than one signalling point, and may therefore be assigned more than one signalling point code.

2.3 All international signalling point codes (ISPC) should consist of three identification sub-fields as indicated in Figure 1/Q.708. The sub-field of 3 bits (NML) should identify a world geographical zone. The sub-field of 8 bits (K-D) should identify a geographical area or network in a specific zone. The sub-field of 3 bits (CBA) should identify a signalling point in a specific geographical area or network. The combination of the first and second sub-fields could be regarded as a signalling area/network code (SANC).

2.4 Each country (or geographical area) should be assigned at least one signalling area/network code (SANC).

2.5 Two of the zone identifications, namely 0 and 1 codes, are reserved for future allocation.

2.6 The system of international signalling point codes (ISPC) will provide for 6 × 256 × 8 (12288) ISPCs.

2.7 If a country (or geographical area) should require more than 8 international signalling points, one or more additional signalling area/network code(s) (SANC) would be assigned to it.

2.8 Lists of signalling area/network codes (SANC) to be used in the development of international signalling point codes (ISPC) is given in Annex A to this Recommendation. It shows SANCs assigned to each geographical area that already has other code assignments in existing public telecommunication networks. All codes not shown on the lists are spare codes.

2.9 The assignment of signalling area/network codes (SANC) is to be administered by the CCITT. The assignment of signalling point identifications in the sub-field (CBA) will be made by each country (or geographical area) and the CCITT Secretariat notified.

2.10 The Member countries of the International Telecommunications Union not mentioned in Annex A who wish to take part in the international signalling network or those Members that require an additional signalling area/network code (SANC) should ask the Director of the CCITT for the assignment of an available SANC. In their request, they may indicate the available SANC preferred.

2.11 The Director of the CCITT takes care that:

- generally the assignments are made on a one by one basis and contiguously for a given geographical area, or a given signalling network. (Geographical designations, or network names, may be entered in the list.)
- the needs of each Member country of the International Telecommunication Union for a new SANC shall be met under all circumstances. Should there not be any additional contiguous codes available, a new sequence of contiguous codes shall be opened up for the country concerned. Such a new code sequence will be established firstly at the bottom of the block of spare codes at the end of the lists in Annex A, and secondly at the bottom of existing sequences when it is likely that the adjacent code groups will not require the spares.
- code assignments appearing in Annex A, but obviously not required anymore because the networks concerned are reached with other SANCs will be deleted from the Annex.

2.12 Assignments by the Director of the CCITT of SANC as well as assignments by countries of the signalling point identifications will be published in the Operational Bulletin of the ITU. The representation of ISPC should be shown in decimal form in each sub-field, i.e. Z-UUU-V where Z, UUU, and V are corresponding to bits NML, K-D and CBA, respectively.

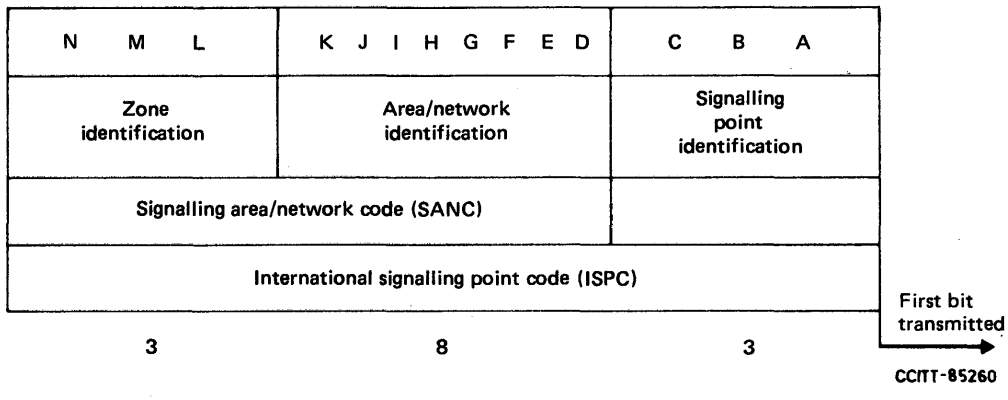



FIGURE 1/Q.708

**Format for international signalling point code (ISPC)**

ANNEX A

(to Recommendation Q.708)

**Lists of Signalling Area/Network Codes (SANC)**

*Note* – These lists are shown by the decimal representation, i.e. Z-UUU where Z is zone identification and UUU is area/network identification.

**Zone 2**

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 2-004 | Greece |
| 2-008 | Netherlands (Kingdom of the) |
| 2-012 | Belgium |
| 2-016 through 2-023 | France |
| 2-024 | Monaco |
| 2-028 | Spain |
| 2-032 | Hungarian People's Republic |
| 2-036 | German Democratic Republic |
| 2-040 | Yugoslavia (Socialist Federal Republic of) |
| 2-044 through 2-046 | Italy |
| 2-052 | Romania (Socialist Republic of) |
| 2-056 | Switzerland (Confederation of) |
| 2-060 | Czechoslovak Socialist Republic |
| 2-064 | Austria |
| 2-068 | United Kingdom of Great Britain and Northern Ireland (British Telecom) |
| 2-072 | United Kingdom of Great Britain and Northern Ireland (Mercury Telecommunications Limited) |
| 2-076 | Denmark |
| 2-080 and 2-081 | Sweden |
| 2-084 | Norway |
| 2-088 | Finland |
| 2-100 | Union of Soviet Socialist Republics |
| 2-120 | Poland (People's Republic of) |
| 2-124 through 2-131 | Germany (Federal Republic of) |
| 2-132 | Gibraltar |
| 2-136 | Portugal |
| 2-140 | Luxembourg |
| 2-144 | Ireland |
| 2-148 | Iceland |
| 2-152 | Albania (Socialist People's Republic of) |
| 2-156 | Malta (Republic of) |
| 2-160 | Cyprus (Republic of) |
| 2-168 | Bulgaria (People's Republic of) |
| 2-172 | Turkey |

Zone 2, Spare Codes: 224

**Zone 3**

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 3-004 | Canada |
| 3-016 | St. Pierre and Miquelon (French Department of) |
| 3-020 through 3-059 | United States of America |
| 3-060 | Puerto Rico |
| 3-064 | Virgin Islands (USA) |

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 3-068, 3-069 and 3-070 | Mexico |
| 3-076 | Jamaica |
| 3-080 | French Antilles |
| 3-084 | Barbados |
| 3-088 | Antigua and Barbuda |
| 3-092 | Cayman Islands |
| 3-096 | British Virgin Islands |
| 3-100 | Bermuda |
| 3-104 | Grenada |
| 3-108 | Montserrat |
| 3-112 | St. Kitts and Nevis |
| 3-116 | St. Lucia |
| 3-120 | St. Vincent and the Grenadines |
| 3-124 | Netherlands Antilles |
| 3-128 | Bahamas (Commonwealth of the) |
| 3-132 | Dominica (Commonwealth of) |
| 3-136 | Cuba |
| 3-140 | Dominican Republic |
| 3-144 | Haiti (Republic of) |
| 3-148 | Trinidad and Tobago |
| 3-152 | Turks and Caicos Islands |
| 3-156 | Guadeloupe |
| 3-160 | Martinique |

Zone 3, Spare Codes: 228

## Zone 4

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 4-008 | India (Republic of) |
| 4-020 | Pakistan (Islamic Republic of) |
| 4-024 | Afghanistan (Democratic Republic of) |
| 4-026 | Sri Lanka (Democratic Socialist Republic of) |
| 4-028 | Burma (Socialist Republic of the Union of) |
| 4-030 | Lebanon |
| 4-032 | Jordan (Hashemite Kingdom of) |
| 4-034 | Syrian Arab Republic |
| 4-036 | Iraq (Republic of) |
| 4-038 | Kuwait (State of) |
| 4-040 | Saudi Arabia (Kingdom of) |
| 4-042 | Yemen (Arab Republic) |
| 4-044 | Oman (Sultanate of) |
| 4-046 | Yemen (People's Democratic Republic of) |
| 4-048 | United Arab Emirates |
| 4-050 | Israel (State of) |
| 4-052 | Bahrain (State of) |
| 4-054 | Qatar (State of) |
| 4-056 | Mongolian People's Republic |
| 4-058 | Nepal |
| 4-060 | United Arab Emirates (Abu Dhabi) |
| 4-062 | United Arab Emirates (Dubai) |
| 4-064 | Iran (Islamic Republic of) |

**Zone 4** *(suite)*

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 4-080 | Japan |
| 4-100 | Korea (Republic of) |
| 4-104 | Viet Nam (Socialist Republic of) |
| 4-108 | Hong Kong |
| 4-110 | Macao |
| 4-112 | Democratic Kampuchea |
| 4-114 | Lao People's Democratic Republic |
| 4-120 | China (People's Republic of) |
| 4-135 | Korea (Democratic People's Republic of) |
| 4-140 | Bangladesh (People's Republic of) |
| 4-144 | Maldives (Republic of) |

Zone 4, Spare Codes: 223

**Zone 5**

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 5-004 | Malaysia |
| 5-010 | Australia |
| 5-020 | Indonesia (Republic of) |
| 5-030 | Philippines (Republic of) |
| 5-040 | Thailand |
| 5-050 | Singapore (Republic of) |
| 5-056 | Brunei Darussalam |
| 5-060 | New Zealand |
| 5-070 | Guam |
| 5-072 | Nauru (Republic of) |
| 5-074 | Papua New Guinea |
| 5-078 | Tonga (Kingdom of) |
| 5-080 | Solomon Islands |
| 5-082 | Vanatu (Republic of) |
| 5-084 | Fiji (Republic of) |
| 5-086 | Wallis and Futuna Islands |
| 5-088 | American Samoa |
| 5-090 | Niue Island |
| 5-092 | New Caledonia and Dependencies |
| 5-094 | French Polynesia |
| 5-096 | Cook Islands |
| 5-098 | Western Samoa (Independent State of) |
| 5-100 | Kiribati (Republic of) |
| 5-102 | Tuvalu |

Zone 5, Spare Codes: 232

## Zone 6

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 6-004 | Egypt (Arab Republic of) |
| 6-006 | Algeria (Algerian Democratic and Popular Republic) |
| 6-008 | Morocco (Kingdom of) |
| 6-010 | Tunisia |
| 6-012 | Libya (Socialist People's Libyan Arab Jamahiriya) |
| 6-014 | Gambia (Republic of the) |
| 6-016 | Senegal (Republic of the) |
| 6-018 | Mauritania (Islamic Republic of) |
| 6-020 | Mali (Republic of) |
| 6-022 | Guinea (Republic of) |
| 6-024 | Côte d'Ivoire (Republic of the) |
| 6-026 | Burkina Faso |
| 6-028 | Niger (Republic of the) |
| 6-030 | Togolese Republic |
| 6-032 | Benin (People's Republic of) |
| 6-034 | Mauritius |
| 6-036 | Liberia (Republic of) |
| 6-038 | Sierra Leone |
| 6-040 | Ghana |
| 6-042 | Nigeria (Federal Republic of) |
| 6-044 | Chad (Republic of) |
| 6-046 | Central African Republic |
| 6-048 | Cameroon (Republic of) |
| 6-050 | Cape Verde (Republic of) |
| 6-052 | Sao Tome and Principe (Democratic Republic of) |
| 6-054 | Equatorial Guinea (Republic of) |
| 6-056 | Gabon Republic |
| 6-058 | Congo (People's Republic of the) |
| 6-060 | Zaire (Republic of) |
| 6-062 | Angola (People's Republic of) |
| 6-064 | Guinea-Bissau (Republic of) |
| 6-066 | Seychelles (Republic of the) |
| 6-068 | Sudan (Republic of the) |
| 6-070 | Rwanda (Republic of) |
| 6-072 | Ethiopia (People's Democratic Republic of) |
| 6-074 | Somali Democratic Republic |
| 6-076 | Republic of Djibouti |
| 6-078 | Kenya (Republic of) |
| 6-080 | Tanzania (United Republic of) |
| 6-082 | Uganda (Republic of) |
| 6-084 | Burundi (Republic of) |
| 6-086 | Mozambique (People's Republic of) |
| 6-090 | Zambia (Republic of) |
| 6-092 | Madagascar (Democratic Republic of) |
| 6-094 | Reunion (French Department of) |
| 6-096 | Zimbabwe (Republic of) |
| 6-098 | Namibia |
| 6-100 | Malawi |
| 6-102 | Lesotho (Kingdom of) |
| 6-104 | Botswana (Republic of) |
| 6-106 | Swaziland (Kingdom of) |
| 6-108 | Comoros (Islamic Federal Republic of the) |
| 6-110 | South Africa (Republic of) |

Zone 6, Spare Codes: 203

## Zone 7

| *Code* | *Geographical Area or Signalling Network* |
|---|---|
| 7-004 | Belize |
| 7-008 | Guatemala (Republic of) |
| 7-012 | El Salvador (Republic of) |
| 7-016 | Honduras (Republic of) |
| 7-020 | Nicaragua |
| 7-024 | Costa Rica |
| 7-028 | Panama (Republic of) |
| 7-032 | Peru |
| 7-044 | Argentine Republic |
| 7-048 | Brazil (Federative Republic of) |
| 7-060 | Chile |
| 7-064 | Colombia (Republic of) |
| 7-068 | Venezuela (Republic of) |
| 7-072 | Bolivia (Republic of) |
| 7-076 | Guyana |
| 7-080 | Ecuador |
| 7-084 | Guiana (French Department of) |
| 7-088 | Paraguay (Republic of) |
| 7-092 | Suriname (Republic of) |
| 7-096 | Uruguay (Eastern Republic of) |

Zone 7, Spare Codes: 236

**Recommendation Q.709**

### HYPOTHETICAL SIGNALLING REFERENCE CONNECTION

#### 1 Introduction

This Recommendation specifies how the elements of a signalling connection are combined to meet the signalling requirements of the networks that it supports. Included are parameters for signalling transfer delay in both national and international networks, and overall signalling delay that such combinations will produce, together with the availability required, to enable the performance of the network served by the signalling network to be maintained.

A probabilistic approach is been taken, i.e., limits are specified for mean and 95% of connections. These figures will apply to the normal operation of a signalling network. No consideration is given to the "unusually long" signalling paths that are found in some signalling networks. Any unusual routing caused by some network structures and/or reconfigurations due to network failure are considered to be covered in the remaining 5% of connections.

The hypothetical signalling reference connection (HSRC) for international working is specified in this Recommendation by defining the constituent parts of:

i) the international section,

ii) the national section.

In any combination of those sections to produce an overall hypothetical signalling reference connection, it is necessary to consider what impact each of the component parts (international and two national sections) have on each other and the full hypothetical signalling reference connection. This means that certain national or international limits such as the maximum number of signalling transfer points allowed in a signalling relation (see Recommendation Q.705, § 5.2) require modification and account of this has been taken in this Recommendation.

## 2 Requirements of networks served by the signalling connection

To meet the requirements of services carried on the network served by the signalling network, the signalling connection performance should be closely aligned with those requirements. Since these services are ultimately to be carried on an ISDN, the hypothetical signalling reference connection is based upon the hypothetical reference connection produced for that network (Recommendation G.801).

However, for a considerable time the majority of services in the network served by the signalling network will be telephony-based and account must therefore be taken of the reference connection for conventional telephony application (Recommendation G.101).

## 3 Hypothetical signalling reference connection components for link-by-link signalling

### 3.1 *General*

The components of an hypothetical signalling reference connection are signalling points and STPs which are connected in series by signalling data links to produce a signalling connection (Note 1). The number of signalling points and STPs depend on the size of the network. Two limits are prescribed to cover mean or 95% cases. Separate cases are allowed for large countries and average sized countries (Note 2). This section outlines the considerations involved in formulating a hypothetical signalling reference connection for link-by-link signalling and details the number of hypothetical signalling reference connection components and the delays they produce.

*Note 1* – The term signalling point is used to designate use of the user function in a signalling point: whether or not STP function is presented irrelevant in this context. The term STP is used to designate use of the STP function in a signalling point: whether or not user function is present is irrelevant in this context.

*Note 2* – When the maximum distance between an international switching centre and a subscriber who can be reached from it does not exceed 1000 km or, exceptionally, 1500 km, and when the country has less than $n \times 10^7$ subscribers, the country is considered as of average size. A country with a larger distance between an international switching centre and a subscriber, or with more than $n \times 10^7$ subscribers, is considered as of large size. (The value of $n$ is for further study.)

#### 3.1.1 *Number of signalling points in the hypothetical signalling reference connection*

The number of signalling points in the hypothetical signalling reference connection has been determined by considering the maximum number of links allowed by the Telephone Routing Plan (Q.13/E.171). These Recommendations define "last choice" backbone routes and only a small proportion of traffic take these routes. Traffic generated in metropolitan areas, generally the largest source of traffic, usually takes far fewer links to an international switching centre. Even for rural areas a connection to the international switching centre will not generally be required to follow the backbone route.

Limitation of the number of signalling points required will reduce the signalling delay, considering that signalling point delay, forms the largest component of signalling delay.

#### 3.1.2 *Number of STPs in an hypothetical signalling reference connection*

The number of STPs in the hypothetical signalling reference connection is a function of the number of signalling points, and the signalling network topology used to connect these signalling points. The number of STPs should be kept to a minimum in order to limit the signalling delay. In some signalling relationship, associated signalling may be used for which no STPs are required. In others, one or more STPs may be used. For international signalling relationship, it is recommended that no more than 2 STPs be used in a signalling relation. (See Recommendation Q.705, § 5.2.)

#### 3.1.3 *Signalling network availability*

The availability of a signalling connection is an important network parameter. It is necessary for the availability to be significantly better than the availability of the component being controlled (e.g. a circuit). A figure of 10 minutes down time per year maximum unavailability is recommended for any particular signalling route set (Recommendation Q.706, § 1.1).

This corresponds to an availability of 0.99998, which can be achieved by the use of suitable network redundancies.

3.1.4 *Signalling message transfer delay*

Signalling message transfer delay is another important network parameter. It affects call set up delay and also affects network response time to service requests made during a call. In this Recommendation, the transmission propagation delays are not included (see § 7.2).

3.2 *International component of hypothetical signalling reference connection*

The international component of the hypothetical signalling reference connection includes all international signalling points in the connection and the STPs carrying signalling messages between the signalling points. The maximum number of signalling points and STPs allowed are listed in Table 1/Q.709.

The unavailability of the overall international component of the signalling network should not exceed the following totals per year for both the 50 and 95 percent cases.

- 20 minutes for large country to large country,
- 30 minutes for large country to average-sized country, and
- 40 minutes per year for average-sized country to average-sized country.

TABLE 1/Q.709

**Maximum number of signalling points and STPs in international component**

| Country size (Note) | Percent of connections | Number of STPs | Number of signalling points |
|---|---|---|---|
| Large to Large | mean | 3 | 3 |
| | 95 | 4 | |
| Large to Average-sized | mean | 4 | 4 |
| | 95 | 5 | |
| Average-sized to Average-sized | mean | 5 | 5 |
| | 95 | 7 | |

*Note* – See Note 2 to § 3.1.

The maximum signalling transfer delay under normal conditions for the international component of a connection should not be worse than the values listed in Table 2/Q.709.

3.3 *National components of hypothetical signalling reference connection*

The national components of the hypothetical signalling reference connection includes all national exchanges in the connection (but does not include the international switching centre in the country) and all STPs carrying signalling messages between the national exchanges and between the highest level national exchange and the international switching centre. The maximum number of signalling points and STPs allowed are listed in Table 3/Q.709.

TABLE 2/Q.709

**Maximum signalling delays for international component**

| Country size | Percent of connections | Delay (Note) (ms) | |
|---|---|---|---|
| | | Message type | |
| | | Simple (e.g. answer) | Processing intensive (e.g. IAM) |
| Large to Large | mean | 390 | 600 |
| | 95 | 410 | 620 |
| Large to Average-sized | mean | 520 | 800 |
| | 95 | 540 | 820 |
| Average-sized to Average-sized | mean | 650 | 1000 |
| | 95 | 690 | 1040 |

*Note* – Only the mean delay component from Table 4/Q.706, Table 3/Q.725 and Table 1/Q.766 have been used in calculating the delay. Further study is required, e.g. for the mean values as well as the inclusion of overload and/or 95 percentile cases of each component value.

TABLE 3/Q.709

**Maximum number of signalling points and STPs in national components**

| Country size (Note 1) | Percent of connections | Number of STPs | Number of signalling points |
|---|---|---|---|
| Large | mean | 3 | 3 |
| | 95 | 4 | 4 |
| Average-sized | mean | 2 | 2 |
| | 95 | 3 | 3 |

*Note 1* – See Note 2 to § 3.1.

*Note 2* – The values in this Table are provisional. (A higher number of signalling points and/or STPs might be included in a national network, e.g. in the case that a two-level hierarchical signalling network is adopted. This matter is for further study.)

The unavailability of each of the overall national components of the signalling network should not exceed the following totals per year:

- 20 minutes for mean case of average-sized countries,
- 30 minutes for 95 percent case of average-sized countries and mean case of large countries, and
- 40 minutes for 95 percent case of large countries.

*Note 1* – Although the signalling component of the international switching centre in the country was not included in Table 3/Q.709, it is included in the unavailability objectives.

*Note 2* – The hypothetical signalling reference connection define a unique path through the national and international networks, therefore when considering the overall unavailability of each national component, no account is taken of any standby path, if provided, in that national network. The values given are based on those for each component route-set as specified in Recommendation Q.706, § 1.1. They are provisional and for further study.

The maximum signalling transfer delay under normal conditions for each of the national components of a connection should not be worse than the values listed in Table 4/Q.709.

TABLE 4/Q.709

**Maximum signalling delays for each national component**

| Country size | Percent of connections | Delay (Notes 1 and 2) (ms) | |
|---|---|---|---|
| | | Message type | |
| | | Simple (e.g. answer) | Processing intensive (e.g. IAM) |
| Large | mean | 390 | 600 |
| | 95 | 520 | 800 |
| Average-sized | mean | 260 | 400 |
| | 95 | 390 | 600 |

*Note 1* – See Note to Table 2/Q.709.

*Note 2* – The delay does not include any delay for the International Switching Centre in the country, which is included in the international component.

## 4 Overall signalling delay for link-by-link signalling

From the hypothetical signalling reference connection and the values of message transfer times given for signalling point and STP, the overall signalling delay due to signalling point, and STP delays can be determined from Tables 2 and 4 of this Recommendation, for a given load in a given network. Average delays and 95 percentile delays are given in Table 5/Q.709 for various combinations of large and average-sized countries. Average signalling point and STP delays at normal loading are assumed.

These values must be increased by the transmission propagation delays (see Table 1/Q.41).

TABLE 5/Q.709

**Maximum overall signalling delays**

| Country size | Percent of connections | Delay (Note) (ms) | |
|---|---|---|---|
| | | Message type | |
| | | Simple (e.g. answer) | Processing intensive (e.g. IAM) |
| Large to Large | mean | 1170 | 1800 |
| | 95 | 1450 | 2220 |
| Large to Average-sized | mean | 1170 | 1800 |
| | 95 | 1450 | 2220 |
| Average to Average-sized | mean | 1170 | 1800 |
| | 95 | 1470 | 2240 |

*Note* – See Note to Table 2/Q.709.

## 5 Hypothetical signalling reference connection (HSRC) components for end-to-end signalling

### 5.1 *General*

The components of a hypothetical signalling reference connection are signalling end points (SEP), signalling points with SCCP relay function (SPR) and STPs which are connected in series by signalling data links to produce an end-to-end signalling connection (Note 1). The number of the various signalling nodes depends on the size of the network. Two limits are prescribed to cover mean or 95% cases. Separate cases are allowed for large countries and average-sized countries (Note 2). This section outlines the considerations involved in formulating a hypothetical signalling reference connection and details the number of hypothetical signalling reference connection components and the delays they produce.

*Note 1* – a) Signalling End Point (SEP) – This includes processing in UP/AP (User part/application part), SCCP (Signalling connection control part), MTP (Message transfer part) and also MTP-SCCP-UP/AP

b) Signalling Point with SCCP relay function (SPR) – This includes only processing in MTP-SCCP-MTP

c) Signalling Transfer Point – This includes processing in MTP exclusively.

*Note 2* – When the maximum distance between an international switching centre and a subscriber who can be reached from it does not exceed 1000 km or, exceptionally, 1500 km, and when the country has less than $n \times 10^7$ subscribers, the country is considered as of average size. A country with a larger distance between an international switching centre and a subscriber, or with more than $n \times 10^7$ subscribers is considered as of large size. (The value of $n$ is for further study.)

5.1.1 *Number of signalling nodes in the end-to-end HSRC*

The same signalling network is used for end-to-end messages and link-by-link messages. This means that the maximum number of signalling nodes is equal in both cases. The maximum number of signalling nodes from the originating node to the destination node is 18 in 50 percent of the connections and 23 in 95 percent of the connections except for average-sized to average-sized country. In that case the value is 24.

In general a fast transfer of end-to-end signalling messages has to be required. For such messages a route with a minimum number of signalling transfer and relay points is highly desirable.

It is desirable to use the message routing of the MTP (STP functions) as far as possible and trying in this way to avoid processing in higher layers (SCCP or user functions).

5.1.2 *Signalling network availability*

The availability of a signalling connection is an important network parameter. It is necessary for the availability to be significantly better than the availability of the component being controlled (e.g. a circuit). A figure of ten minutes down time per year maximum unavailability is recommended for any particular signalling route set (Recommendation Q.706, § 1.1).

This corresponds to an availability of 0.99998, which can be achieved by the use of suitable network redundancies.

5.1.3 *Signalling message transfer delay*

Signalling message transfer delay is another important network parameter. It affects call set up delay and also affects network response time to service requests made during a call.

The use of signalling points with SCCP relay functions (SPR) should be kept to a minimum. In an SPR additional processing is performed which causes an additional delay, for example address translation for CR or UDT message types (processing intensive messages) or a local reference message mapping for CC or DT messages (processing simple message types). The cross office transit time for SPR is defined in Q.716. The cross-office transit time for an SEP is equal to $T_{cu}$ in Q.766 or Q.725 and for an STP is equal to $T_{cs}$ in Q.706.

5.2 *International component of hypothetical signalling reference connection*

The international component of the hypothetical signalling reference connection includes all international signalling nodes (e.g. SPR and STP) in the connection. The maximum number of SPRs and STPs allowed are listed in Table 6/Q.709.

TABLE 6/Q.709

**Maximum number of SPRs and STPs in international component**

| Country size | Percent of connections | Number of STPs | Number of SPRs |
|---|---|---|---|
| Large to Large | mean | 4 | 2 |
| | 95 | 4 | 3 |
| Large to Average-sized | mean | 6 | 2 |
| | 95 | 6 | 3 |
| Average-sized to Average-sized | mean | 8 | 2 |
| | 95 | 8 | 4 |

The unavailability of the overall international component of the signalling network should not exceed the following totals per year for both the 50 and 95 percent cases:

- 20 minutes for large country to large country;
- 30 minutes for large country to average-sized country, and
- 40 minutes per year for average-sized country to average-sized country.

The maximum delay at the signalling nodes under normal conditions for the international component of a connection should not be worse than the values listed in Table 7/Q.709.

TABLE 7/Q.709

**Maximum delay at the signalling nodes for international component**

| Country size | Percent of connections | Delay (ms) | |
|---|---|---|---|
| | | Message type | |
| | | Processing simple | Processing intensive |
| Large to Large | mean | 300 | 440 |
| | 95 | 410 | 620 |
| Large to Average-sized | mean | 340 | 480 |
| | 95 | 450 | 660 |
| Average-sized to Average-sized | mean | 380 | 520 |
| | 95 | 600 | 880 |

*Note 1* – The maximum signalling nodes delay is the sum of all cross-office delays involved.

*Note 2* – All values are provisional.

## 5.3 *National components of hypothetical signalling reference connections*

The national components of the hypothetical signalling reference connection includes all national signalling nodes (e.g., SEP, SPR, STP) in the connection (but does not include the international switching centre in the country). The maximum number of SEPs, SPRs and STPs allowed are listed in Table 8/Q.709.

The unavailability of each of the overall national components of the signalling network should not exceed the following totals per year:

- 20 minutes for mean case of average-sized countries;
- 30 minutes for 95 percent case of average-sized countries and mean case of large countries, and
- 40 minutes for 95 percent case of large countries.

TABLE 8/Q.709

**Maximum number of SEPs, SPRs and STPs in national component**

| Country size | Percent of connections | Number of STPs | Number of SPRs | Number of SEPs |
|---|---|---|---|---|
| Large | mean | 4 | 1 | 1 |
| | 95 | 5 | 2 | 1 |
| Average-sized | mean | 2 | 1 | 1 |
| | 95 | 4 | 1 | 1 |

*Note 1* – Although the signalling component of the international switching centre in the country is not included in Table 8/Q.709, it is included in the unavailability objectives.

*Note 2* – The hypothetical signalling reference connection defines a unique path through the national and international networks, therefore when considering the overall unavailability of each national component, no account is taken of any standby path, if provided, in that national network. The values given are based on those for each component route-set as specified in Recommendation Q.706, § 1.1.

The maximum delay at the signalling nodes under normal conditions for each of the national components of a connection should not be worse than the values listed in Table 9/Q.709.

TABLE 9/Q.709

**Maximum delay at the signalling nodes for each national component**

| Country size | Percent of connections | Delay (ms) | |
|---|---|---|---|
| | | Message type | |
| | | Processing simple | Processing intensive |
| Large | mean | 300 | 440 |
| | 95 | 430 | 640 |
| Average-sized | mean | 260 | 400 |
| | 95 | 300 | 440 |

*Note 1* – The maximum signalling nodes delay is the sum of all cross-office delays involved.

*Note 2* – All values are provisional.

## 6 Overall signalling delay for end-to-end signalling

The link-by-link signalling delay is applicable where messages are processed by each signalling point (e.g. during call establishment). The use of end-to-end signalling intended to reduce the overall signalling delay.

From the hypothetical signalling reference connection and the values of message transfer times given for SEPs, SPRs and STPs, the overall signalling delay due to the node delays can be determined from Tables 7 and 9 of this Recommendation, for a given load in a given network. Average delays and 95 percentile delays are given in Table 10/Q.709 for various combinations of large and average-sized countries. Average signalling node delays at normal loading are assumed.

TABLE 10/Q.709

**Maximum overall delay at the signalling nodes**

| Country size | Percent of connections | Delay (ms) | |
|---|---|---|---|
| | | Message type | |
| | | Processing simple | Processing intensive |
| Large to Large | mean | 900 | 1320 |
| | 95 | 1270 | 1900 |
| Large to Average-sized | mean | 900 | 1320 |
| | 95 | 1180 | 1740 |
| Average-sized to Average-sized | mean | 900 | 1320 |
| | 95 | 1200 | 1760 |

*Note 1* – The maximum signalling nodes delay is the sum of all cross-office delays involved.

*Note 2* – All values are provisional.

## 7 Remarks

7.1 The above values for signalling delays assumes a message length distribution as given in Table 2/Q.706 and Table 2/Q.725, with a mean message length of 15 octets. However, a message length of e.g. 128 octets for SCCP user data in CR and CC messages and 255 octets for SCCP user data in DT messages are permissible. For such a message length the transmission time at 64 kbit/s is, in each signalling node, about 15 ms (128 octets) to 30 ms (255 octets) longer.

7.2 When defining an overall signalling delay the propagation delay must be included. This delay cannot be completely neglected due to the geographical size of the HSRC (see Table 1/Q.41).

**PAGE INTENTIONALLY LEFT BLANK**

**PAGE LAISSEE EN BLANC INTENTIONNELLEMENT**

SECTION 3

# SIMPLIFIED MESSAGE TRANSFER PART

## Recommendation Q.710

### SIMPLIFIED MTP VERSION FOR SMALL SYSTEMS

### 1 Field of application

1.1 This Recommendation is applicable for systems using a simplified MTP version to interface to the public network(s).

1.2 The MTP functions specified in § 3 of this Recommendation may be applied in general for small systems, e.g., PABX's, remote concentrators, etc., interfacing with the message transfer part described in Recommendations Q.702, Q.703, Q.704 and Q.707.

1.3 The Recommendation applies only for digital access arrangements.

1.3.1 In case one channel carries signalling information for more than one multiplex system, at least one additional channel should be pre-assigned as a stand-by signalling link in a multiplex system other than that which contains the active channel. This allows the changeover and changeback procedures specified in §§ 3.4.4 and 3.4.5 to be performed.

1.3.2 The stand-by channel(s) should not be used as B-channel(s).

1.4 Only the associated mode of signalling is applicable.

1.5 A variety of information types may be supported by the signalling system, e.g., relating to circuit switched call control and packet communication.

### 2 Functional content

The functional requirements are as follows:

2.1 The network call control functions are as specified in Recommendation Q.930 (I.451).

*Note* – Different network layer protocols (circuit switching and packet switching) may be supported by using the protocol discriminator included in Recommendation Q.930. As an alternative, different network layer entities may access the interface functions directly. In that case, the interface functions will use separate service indicator codes to discriminate the applicable network layer entity. This will be similar to the use of SAPI specified in Recommendation Q.920. Which principle to be applied is determined by the Administration/RPOA.

2.2 The minimum set of Message Transfer Part functions are specified in Recommendations Q.702, Q.703, Q.704 and Q.707, with the qualifications specified in § 3 of this Recommendation.

2.3 The additional interface functions required for the proper operation of the D-channel call control functions in combination with the message transfer part functions, are specified in § 4 of this Recommendation (see Figure 1/Q.710).

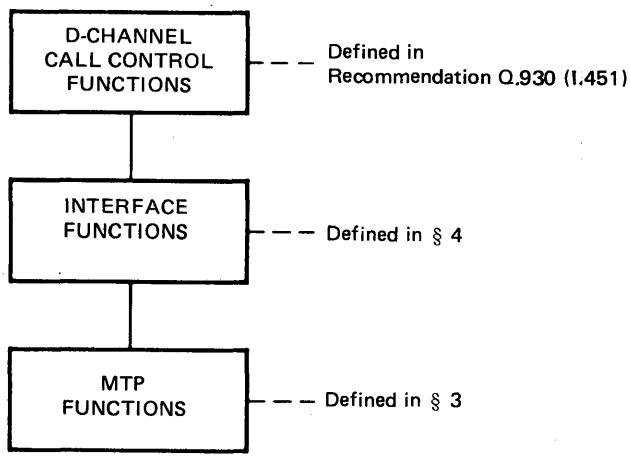



FIGURE 1/Q.710

## 3 Message Transfer Part (MTP) functions

### 3.1 *General*

The MTP functions as specified in Recommendations Q.702, Q.703, Q.704 and Q.707 are applicable. However, the following exceptions and modifications to those Recommendations may be applied for the PABX system, see §§ 3.2-3.4.

In order to prevent fraudulent use of the signalling network, it has to be ensured that no signalling messages generated by a PABX can be routed further than the public exchange to which the PABX has access. The manner in which this is made may be dependent on national circumstances and system implementations. An example of how such a function could be implemented is given in § 3.5.

### 3.2 *Level 1* (Recommendation Q.702)

Only digital signalling data links are relevant. Recommendation Q.702, § 6, is not applicable.

### 3.3 *Level 2* (Recommendation Q.703)

#### 3.3.1 *Initial alignment procedure* (Recommendation Q.703, § 7)

In the initial alignment procedure specified in Recommendation Q.703, § 7, only the emergency proving is applicable. Thus, in states "aligned" and "proving" of the initial alignment procedure status indication "N" is not sent.

#### 3.3.2 *Processor outage* (Recommendation Q.703, § 8)

The processor outage function specified in Recommendation Q.703, § 8, is not applicable.

When the level 2 function receives an indication that a processor outage situation exists at the remote and (through the reception of status signal units indicating processor outage), it transmits status signal units indicating "out of service".

3.3.3 *Flow control* (Recommendation Q.703, § 9)

The sending of the link status indication "B" from the PABX is not applicable.

When the level 2 function of the PABX receives the link status indication "B", no action is taken by the PABX.

3.4 *Level 3* (Recommendation Q.704)

3.4.1 *Routing label* (Recommendation Q.704, § 2.2)

The signalling link selection (SLS) field defined in § 2.2.4 is always coded 0000.

3.4.2 *Message routing function* (Recommendation Q.704, § 2.3)

The load sharing function between link sets and within a link set defined in § 2.3.2 is not applicable.

3.4.3 *Message discrimination* (Recommendation Q.704, § 2.4)

The discrimination function defined in § 2.4.1 is not applicable.

3.4.4 *Changeover* (Recommendation Q.704, § 5)

Changeover between link sets is not applicable.

Initiation of changeover at the reception of a changeover order from the remote end of a link is not applicable (c.f. Recommendation Q.704, § 3.2.2).

The buffer updating procedure defined in § 5.4 is not applicable.

At reception of a changeover order (or emergency changeover order) an emergency changeover acknowledgement is sent in response.

The message retrieval procedure defined in § 5.5 is not applicable.

Diversion of traffic is performed at expiry of a time-out T1 (c.f. Recommendation Q.704, § 16.8) is started when the changeover is initiated.

3.4.5 *Changeback* (Recommendation Q.704, § 6)

Changeback between link sets is not applicable.

The sequence control procedure defined in § 6.3 is not applicable. At reception of a changeback declaration, a changeback acknowledgement is sent in response.

For the purpose of ensuring message sequence integrity, the time controlled diversion procedure specified in § 6.4 is used.

3.4.6 *Forced rerouting* (Recommendation Q.704, § 7)

Forced rerouting is not applicable.

3.4.7 *Controlled rerouting* (Recommendation Q.704, § 8)

Controlled rerouting is not applicable.

3.4.8 *Signalling point restart* (Recommendation Q.704, § 9)

Signalling point restart is not applicable.

3.4.9 *Management inhibiting* (Recommendation Q.704, § 10)

Management inhibiting is not applicable.

3.4.10 *Signalling traffic flow control* (Recommendation Q.704, § 11)

Signalling route set congestion (Recommendation Q.704, § 11.2.3) is not applicable.

MTP User flow control (Recommendation Q.704, § 11.2.7) is not applicable.

3.4.11 *Signalling link management* (Recommendation Q.704, § 12.2)

Only basic link management procedures are applicable.

3.4.12 *Link set activation* (Recommendation Q.704, § 12.2.4)

Link set normal activation defined in § 12.2.4.1 is not applicable.

Link set emergency restart is used in all cases.

3.4.13 *Transfer prohibited* (Recommendation Q.704, § 13.2)

The transfer prohibited function is not applicable. At the reception of a TFP message, no action should be taken.

3.4.14 *Transfer allowed* (Recommendation Q.704, § 13.3)

The transfer allowed function is not applicable. At the reception of a TFA-message, no action should be taken.

3.4.15 *Transfer restricted* (Recommendation Q.704, § 13.4)

The transfer restricted function is not applicable for the PABX. At the reception of the TFR message no action is taken by the PABX.

3.4.16 *Signalling-route-set-test* (Recommendation Q.704, § 13.5)

The signalling-route-set-test procedure is not applicable.

3.4.17 *Transfer controlled* (Recommendation Q.704, §§ 13.7, 13.8)

The transfer controlled function is not applicable for the PABX. At the reception of the TFC message, no action is taken by PABX.

3.4.18 *Signalling route-set-congestion-test* (Recommendation Q.704, § 13.9)

The signalling route-set-congestion-test function is not applicable for the PABX.

At the reception of signalling-route-set-congestion-test message no action is taken by the PABX.

3.4.19 *Signalling link test* (Recommendation Q.707, § 2.2)

The ability to respond to a signalling link test message with a signalling link test acknowledge message must always be provided by the PABX.

3.5 *Example of "Screening Function"*

*Note* – This paragraph is provided for illustration purposes only.

At an exchange (which has the capability of acting as an STP) each message received on a PABX access link is passed through a "screening function" that checks that the DPC of the message is the same as the SP code of the exchange. If that is the case, the message is sent to the normal MTP message handling functions. Otherwise, the message is discarded.

## 4 Interface functions

### 4.1 *General*

The task of the interface functions is to provide the layer-to-layer interfaces according to what is specified in Recommendations Q.920, Q.930 on the one hand and in Recommendation Q.704 on the other, see the Figure 2/Q.710. This will include some conversion functions which are specified in § 4.4.

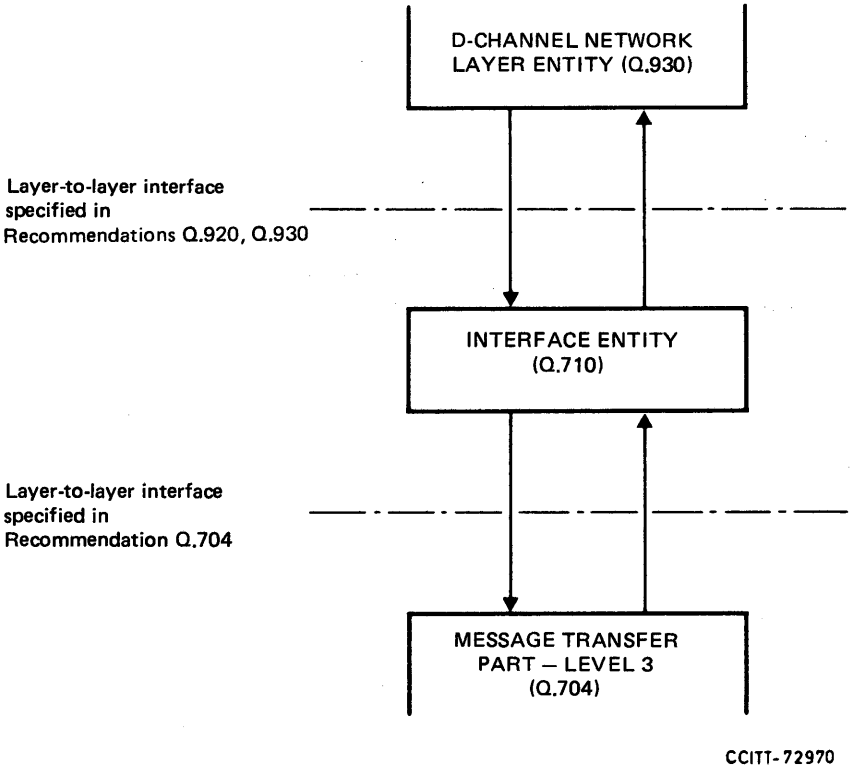



FIGURE 2/Q.710

### 4.2 *Interactions with the network layer entity (Q.930)*

The layer-to-layer interactions between the network layer and the data link layer of the D-channel protocol are specified in Recommendation Q.920, § 4. The interactions are specified in the form of primitives. The primitive applicable for the primary rate interface structure are:

DL-DATA-REQUEST/INDICATION

The DL-DATA-REQUEST primitive is used to request that a network layer message unit be sent. The DL-DATA-INDICATION indicates the arrival of a message unit.

### 4.3 *Interactions with the message transfer part*

The layer-to-layer interactions between the MTP and the User Parts of Signalling System No. 7 are specified in Recommendations Q.701 and Q.704, Figures 23/Q.704 and 27/Q.704.

The following primitives are used:

a) MTP-TRANSFER (see Recommendation Q.701, § 8.1),

b) MTP-PAUSE (see Recommendation Q.701, § 8.2),

c) MTP-RESUME (see Recommendation Q.701, § 8.3).

## 4.4 *Conversion functions*

The Table 1/Q.710 shows the association between the D-channel primitives and the Signalling System No. 7 interactions.

TABLE 1/Q.710

| | D-channel | SS No. 7 |
|---|---|---|
| Information transfer | DL-DATA | MTP-TRANSFER |
| Flow control | –<br>– | MTP-PAUSE (STOP)<br>MTP-RESUME (START) |

### 4.4.1 *Information transfer*

When receiving a DL-DATA-REQUEST primitive from the network layer entity, the interface entity generates a MTP-TRANSFER Request primitive which contains:

- The message unit associated with the primitive.
- A label consisting of DPC, OPC and SLS. The label is generated by the interface entity on the basis of information regarding the destination of the message. The SLS is coded 0000.

  *Note* – In some implementations where the label is not used for routing purposes, the entire label may be coded "all zeros".
- A service information octet (SIO) is generated by the interface entity in accordance with a predetermined rule and, as a national option, on the basis of priority information associated with the primitive. The NI is coded 10 or 11. The SI code is determined by the Administration or RPOA.

  *Note* – In the case when the interface functions provide direct access to more than one network layer entity, the SI code will depend on the network layer entity to which the message is associated.

When receiving a MTP-TRANSFER Indication from the MTP, the interface entity sends a DL-DATA-INDICATION primitive to the network layer entity.

### 4.4.2 *Flow control*

When receiving a MTP-PAUSE indication from the MTP, the interface entity will generate a DL-PAUSE-INDICATION primitive to the network layer entity.

When receiving a MTP-RESUME indication from the MTP, the interface entity will generate a DL-RESUME-INDICATION primitive to the network layer entity.

SECTION 4

# SIGNALLING CONNECTION CONTROL PART (SCCP)

**Recommendation Q.711**

## FUNCTIONAL DESCRIPTION OF THE SIGNALLING CONNECTION CONTROL PART

### 1 Introduction

#### 1.1 *General*

The Signalling Connection Control Part (SCCP) provides additional functions to the Message Transfer Part (MTP) to cater for both connectionless as well as connection-oriented network services to transfer circuit related and non-circuit related signalling information and other type of information between exchanges and specialized centres in telecommunication networks (e.g., for management and maintenance purposes) via a Signalling System No. 7 network.

A functional block situated above the Message Transfer Part, the latter being described in Recommendations Q.701 through Q.707, performs the functions and procedures of the SCCP. Thus the Message Transfer Part remains unchanged (Figure 1/Q.711). The combination of the MTP and the SCCP is called Network Service Part (NSP).

The Network Service Part meets the requirements for Layer 3 services as defined in the OSI-Reference Model, CCITT Recommendation X.200.

#### 1.2 *Objectives*

The overall objectives of the Signalling Connection Control Part are to provide the means for:

a) logical signalling connections within the CCITT No. 7 Signalling Network;

b) a transfer capability for Signalling Data Units with or without the use of logical signalling connections.

Functions of the SCCP are also used for the transfer of circuit related and call related signalling information of the ISDN User Part with or without setup of end-to-end logical signalling connections. These functions are described in Recommendations Q.714 and Q.764. Figure 1/Q.711 illustrates the embedding of the SCCP within the CCITT No. 7 signalling system.

#### 1.3 *General characteristic*

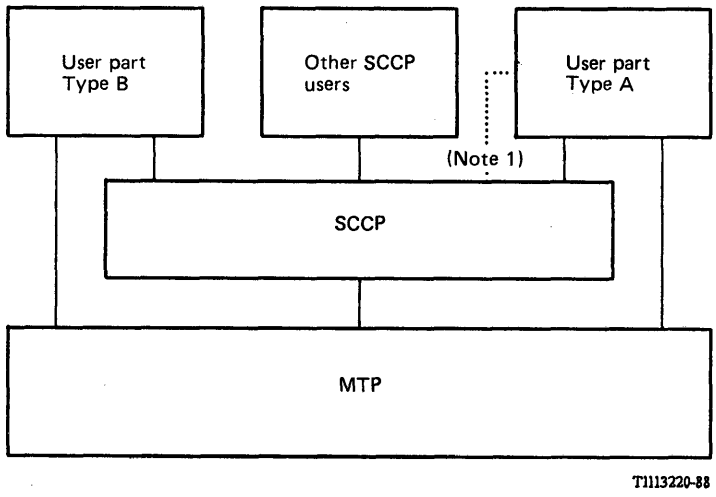
##### 1.3.1 *Technique of description*

The Signalling Connection Control Part (SCCP) is described in terms of:

- services provided by the SCCP,
- services assumed from the MTP,
- functions of the SCCP.

The functions of the SCCP are performed by means of the SCCP-protocol between two systems which provide the NSP-service to the upper layers.

The service interfaces to the upper layers and to the MTP are described by means of primitives and parameters, as recommended in CCITT Recommendation X.200. Figure 2/Q.711 illustrates the relationship between the SCCP protocol and the adjacent services.




*Note 1* – Functional interface.

*Note 2* – The ISDN-UP as defined in Recommendation Series Q.761 to Q.764 is a Type A user part.
– No Type B user parts have yet been specified in CCITT.

FIGURE 1/Q.711

**Functional diagram for the SCCP in CCITT No. 7 Signalling System**

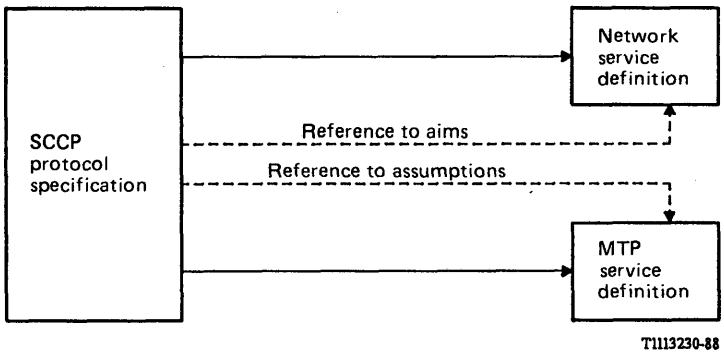



FIGURE 2/Q.711

**Relationship between the SCCP protocol and adjacent services**

1.3.2 *Primitives*

Primitives consist of commands and their respective responses associated with the services requested of the SCCP and of the MTP, see Figure 3/Q.711. The general syntax of a primitive is specified in Recommendation Q.700.

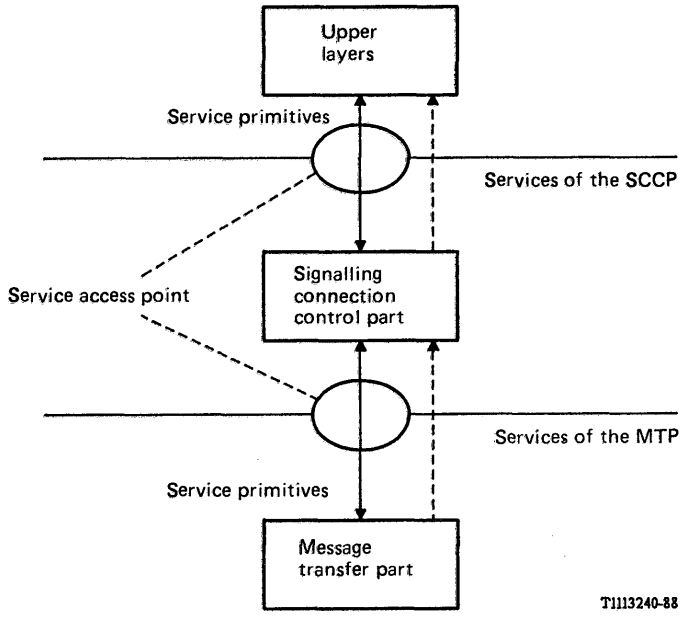



FIGURE 3/Q.711

**Service primitives**

1.3.3 *Peer-to-peer communication*

Exchange of information between two peers of the SCCP is performed by means of a protocol. The protocol is a set of rules and formats by which the control information (and user data) is exchanged between the two peers. The protocol caters for:

- the setup of logical signalling connections,
- the release of logical signalling connections,
- the transfer of data with or without logical signalling connections.

A signalling connection is modelled in the abstract by a pair of queues. The protocol elements are objects on that queue added by the origination SCCP user and removed by the destination SCCP user. Each queue represents a flow control function. Figure 4/Q.711 illustrates the modes described above. (Model for the connectionless service is for further study.)

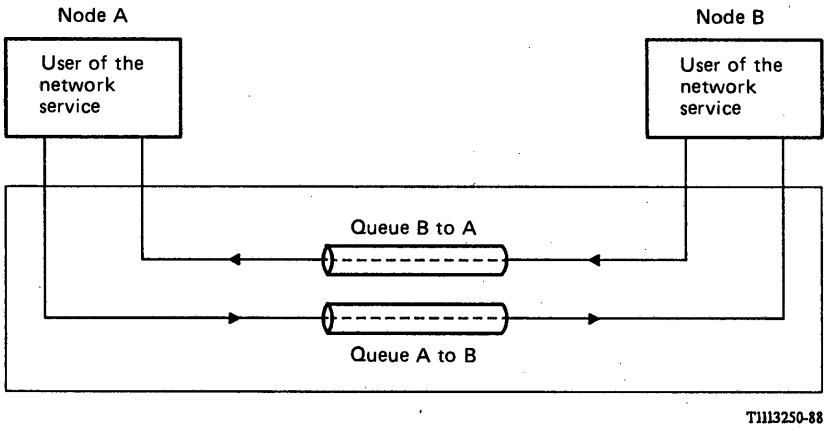



FIGURE 4/Q.711

**Model for the internode communication with the SCCP (Connection-oriented services)**

1.3.4 *Contents of the Recommendations Series Q.71x*

Recommendation Q.711 contains a general description of the services provided by the MTP, the services provided by the SCCP and the functions within the SCCP.

Recommendation Q.712 defines the set of protocol elements and their embedding into messages.

Recommendation Q.713 describes the formats and codes used for the SCCP messages.

Recommendation Q.714 is a detailed description of the SCCP procedures as a protocol specification.

Recommendation Q.716 defines and specifies values for the SCCP performance parameters, including quality of service parameters and internal parameters.

## 2 Services provided by the SCCP

The overall set of services is grouped into:

- connection-oriented services,
- connectionless services.

Four classes of service are provided by the SCCP protocol, two for connectionless services and two for connection-oriented services.

The four classes are:

0 Basic connectionless class

1 Sequenced (MTP) connectionless class

2 Basic connection-oriented class

3 Flow control connection-oriented class

## 2.1 *Connection-oriented services*

A distinction has to be made between:

- temporary signalling connections,
- permanent signalling connections.

Temporary signalling connection establishment is initiated and controlled by the SCCP user. Temporary signalling connections are comparable with dialled telephone connections.

Permanent signalling connections are established and controlled by the local (or remote) O&M-function or by the management function of the node and they are provided for the SCCP user on a semipermanent basis. They can be compared with leased telephone lines.

### 2.1.1 *Temporary signalling connections*

#### 2.1.1.1 *Description*

The control of a signalling connection is divided into the following phases:

- connection establishment phase,
- data transfer phase,
- connection release phase.

##### 2.1.1.1.1 *Connection establishment phase*

Connection establishment procedures provide the mechanism for establishing temporary signalling connections between users of the SCCP.

A signalling connection between two SCCP users may consist of one or more connection sections.

During connection establishment, routing functions are provided by the SCCP, in addition to those provided by the MTP.

At intermediate nodes, SCCP routing determines whether a signalling connection should be realized by one connection or by several concatenated connection sections.

The ISDN UP may provide the routing of the request for the setup of a connection section.

The connection refusal procedure is invoked if the SCCP is unable to establish a signalling connection.

##### 2.1.1.1.2 *Data transfer phase*

The data transfer service provides for an exchange of user data, called Network Service Data Units (NSDU), in either direction or in both directions simultaneously on a signalling connection.

A SCCP message between two peer consists of:

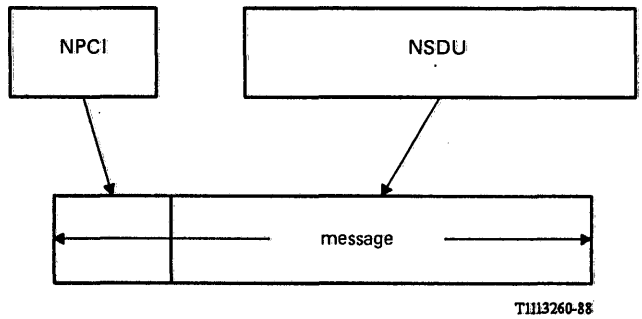
- Network Protocol Control Information (NPCI),
- Network Service Data Unit (NSDU).

The Network Protocol Control Information supports the joint operating of the SCCP-peer entities within the two nodes communicating with each other. It contains a connection reference parameter which allocates the message to a certain signalling connection.

The Network Service Data Unit contains a certain amount of information from the SCCP user which has to be transferred between two nodes using the service of the SCCP.

Network Protocol Control Information and Network Service Data Unit are put together and transferred as a message (Figure 5/Q.711). If the size of user data is too big to be transferred within one message, user data are segmented into a number of portions. Each portion is mapped to a separate message, consisting of the NPCI and a NSDU (Figure 6/Q.711).

The data transfer service caters for sequence control and flow control depending on the quality of service required by the SCCP user (two different classes of the connection-oriented service are provided by the protocol; see Recommendation Q.714).




NPCI = Network protocol control information
NSDU = Network service data unit
message = Protocol data unit

FIGURE 5/Q.711

**Relation between NSDU and message neither segmenting nor blocking**

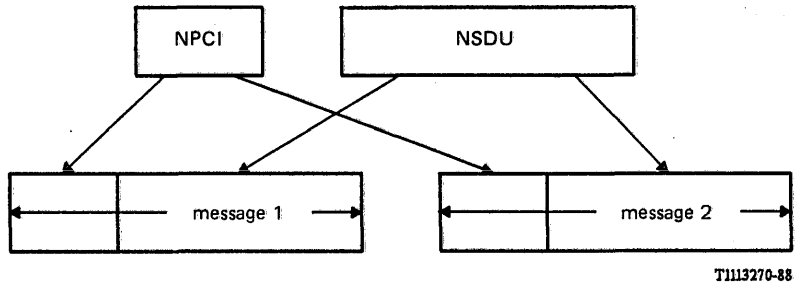



FIGURE 6/Q.711

**Segmenting**

2.1.1.1.3 *Connection release phase*

Connection release procedures provide the mechanism for disconnecting temporary signalling connections between users of the SCCP.

2.1.1.2 *Network service primitives and parameters*

2.1.1.2.1 *Overview*

Table 1/Q.711 gives an overview of the primitives to the upper layers and the corresponding parameters for the (temporary) connection oriented network service. Figure 7/Q.711 shows an overview state transition diagram for the sequence of primitives at a connection endpoint, refer to Recommendation X.213, Network Layer Service Definition of Open Systems Interconnection for CCITT application.

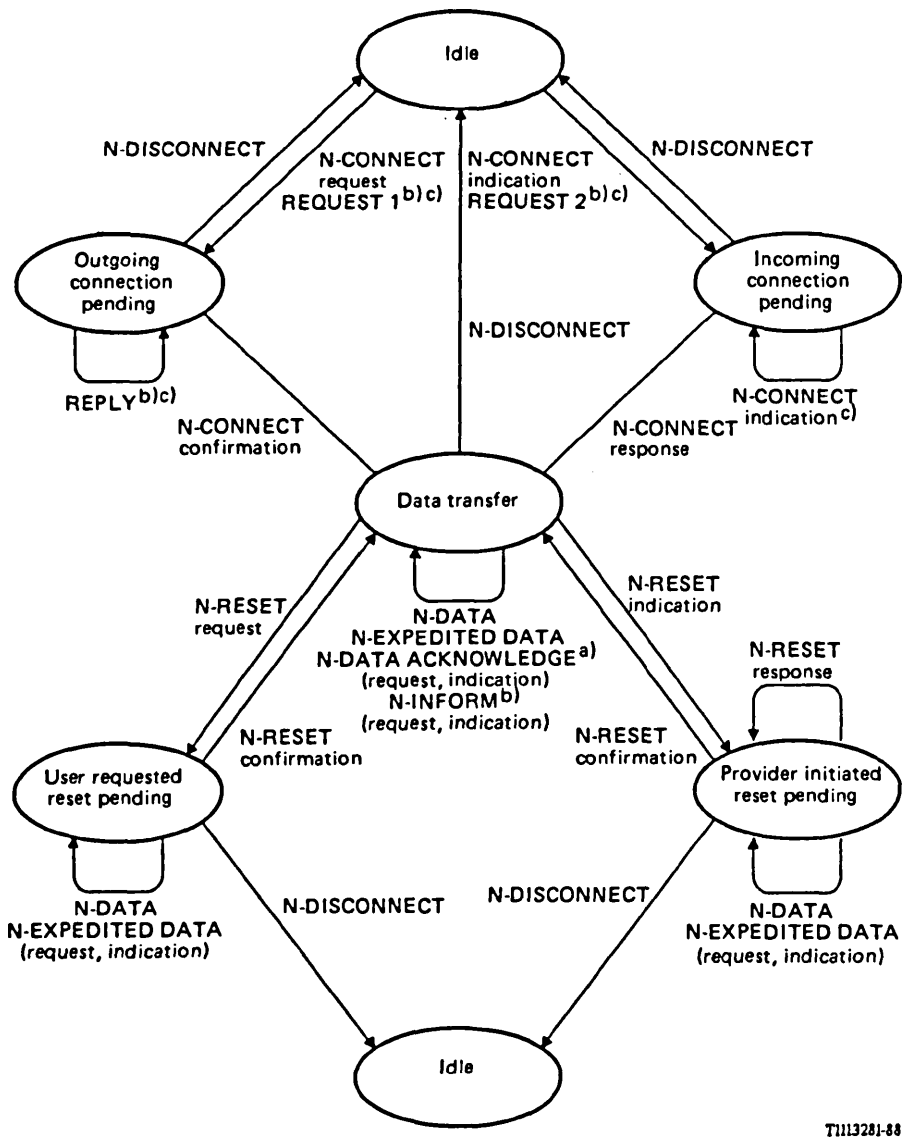
A more detailed description for the primitives and their parameters is given in the following chapters.

TABLE 1/Q.711

**Network service primitives for connection-oriented services**

| Primitives | | Parameters |
|---|---|---|
| Generic name | Specific name | |
| N-CONNECT | Request<br>Indication<br>Response<br>Confirmation | Called address<br>Calling address<br>Responding address<br>Receipt confirmation selection<br>Expedited data selection<br>Quality of service parameter set<br>User data<br>Connection identification [a] |
| N-DATA | Request<br>Indication | Confirmation request<br>User data<br>Connection identification [a] |
| N-EXPEDITED DATA | Request<br>Indication | User data<br>Connection identification [a] |
| N-DATA ACKNOWLEDGE<br>(for further study) | Request<br>Indication | Connection identification [a] |
| N-DISCONNECT | Request<br>Indication | Originator<br>Reason<br>User data<br>Responding address<br>Connection identification [a] |
| N-RESET | Request<br>Indication<br>Response<br>Confirmation | Originator<br>Reason<br>Connection identification [a] |

[a] In Recommendation X.213, § 5.3, this parameter is implicit.




a) The need for this primitive is for further study.

b) This primitive is not in Recommendation X.213. (See Section 2.1.1.3.1.)

c) For user part Type A only.

FIGURE 7/Q.711

*State transition diagram for the sequence of primitives at a connection end-point (basic transitions)*

2.1.1.2.2 *Connection establishment phase*

A SCCP user (calling user) initiates the setup of the connection by means of the primitive "N-CONNECT request" to the SCCP. The SCCP entity evaluates the primitive and adds the protocol control information. The SCCP message (consisting of the protocol control information (PCI) and possibly an NSDU) is transmitted by means of the MTP-services to the remote peer entity of the SCCP. It evaluates and strips the PCI and sends a primitive "N-CONNECT indication" to the local SCCP user. On both ends of the connection the status "pending" is assumed.

The called SCCP user answers with the primitive "N-CONNECT response" to the local SCCP, which sends the response SCCP message including PCI to the calling SCCP. The calling SCCP sends the primitive "N-CONNECT confirmation" to the calling SCCP-User. The connection is now ready for data transfer.

The four types of N-CONNECT, the request, the indication, the response and the confirmation contain the parameters as shown and further described in Table 2/Q.711.

TABLE 2/Q.711

**Parameters of the primitive N-CONNECT**

| Parameter | Primitive | | | |
|---|---|---|---|---|
| | N-CONNECT request | N-CONNECT indication | N-CONNECT response | N-CONNECT confirmation |
| Called address | X | X [d] | | |
| Calling address | X [d] | X | | |
| Responding address | | | X | X |
| Receipt confirmation selection [a] | X | X | X | X |
| Expedited data selection | X | X | X | X |
| Quality of service parameter set | X | X | X | X |
| User data [b] | X | X | X | X |
| Connection identification [c] | X | X | X | X |

X Parameter present within the primitive.

[a] Parameter conditionally present.

[b] User data within the connection primitives are defined as a provider option (refer to CCITT Recommendatiom X.213).

[c] This parameter is not in Recommendation X.213 and is for further study.

[d] This parameter may be implicitly associated with the SCCP service access point at which this primitive is issued.

The parameters "Called address/Calling address" convey addresses identifying the destination/source of a communication. There are three types of addresses:

Global Title,

Subsystem Number,

Signalling Point Code.

The Global Title is an address such as dialled digits which does not explicitly contain information that would allow routing in the signalling network, i.e., a translation function is required. The Subsystem Number is an identification of a specific user function within a certain signalling point (SP), like the ISDN-User Part, the SCCP-Management, etc.

The parameter "Responding address" indicates to which destination the connection has been established or refused.

The "Responding address" parameter in the N-CONNECT primitive conveys the address of the service access point to which the signalling connection has been established. Under certain circumstances (e.g. call redirection, generic addressing, etc.), the value of this parameter may be different from the "Called address" in the corresponding N-CONNECT request. Such facilities that cause the difference are for further study.

The "Responding address" parameter is present in the N-DISCONNECT primitive only in the case where the primitive is used to indicate rejection of a signalling connection establishment attempt by an SCCP user function. The parameter conveys the address of the service access point from which the N-DISCONNECT-request was issued and under circumstances like that mentioned above the "Responding address" may be different from the "Called address" in the corresponding N-CONNECT request primitive.

The parameter "Receipt confirmation selection" indicates the use/availability of the receipt confirmation service. The need for such a service is for further study.

The parameter "Expedited data selection" may be used to indicate during setup whether expedited data can be transferred via the connection. A negotiation will be performed between SCCP users, local and remote.

The Quality of Service parameters are used during call setup to negotiate the protocol class for the connection and, if applicable, the flow control window size.

The N-CONNECT primitives may or may not contain user data.

The parameter "Connection identification" is used to allocate a primitive to a certain connection.

In principle, the connection establishment has to be completed (i.e., data transfer status has to be reached) before sending or receiving data messages. If data messages arrive at the calling user before the connection establishment is finished these data messages are discarded.

In addition, user data can also be transferred to/from the SCCP within the primitives N-CONNECT and N-DISCONNECT.

#### 2.1.1.2.3 *Data transfer phase*

During this phase four different primitives may occur:

a) N-DATA (Table 3/Q.711),

b) N-EXPEDITED DATA (Table 4/Q.711),

c) N-DATA ACKNOWLEDGE,

d) N-RESET (Table 5/Q.711).

The primitive "N-DATA" (Table 3/Q.711) exists only as a "request", i.e. from the SCCP user to the local SCCP and as an "indication" at the remote end of the connection, i.e., from the SCCP to the local SCCP user. N-DATA can occur bidirectionally, i.e., from the calling as well as the called user of the SCCP-connection.

The parameter "Confirmation request" is used in an N-DATA primitive to indicate the need to confirm the receipt of the N-DATA primitive by the remote SCCP user. The confirmation may be given by the N-DATA ACKNOWLEDGE primitive. Receipt confirmation is provided only on connections which get the Receipt Confirmation facility during setup. The matter is for further study.

The primitive "N-EXPEDITED DATA" (Table 4/Q.711) may be used by the SCCP user only, if the signalling connection is set up according to a class providing the capability to transfer expedited data (refer to Recommendation Q.714).

TABLE 3/Q.711

**Parameters of the primitive N-DATA**

| Parameter | Primitive | |
|---|---|---|
| | N-DATA request | N-DATA indication |
| Confirmation request [a] | X | X |
| User data | X | X |
| Connection identification [b] | X | X |

X Parameter present within the primitive.

[a] Parameter conditionally present.

[b] This parameter is for further study.

TABLE 4/Q.711

**Parameters of the primitive N-EXPEDITED DATA**

| Parameter | Primitive | |
|---|---|---|
| | N-EXPEDITED DATA request | N-EXPEDITED DATA indication |
| User data | X | X |
| Connection identification [a] | X | X |

X Parameter present within the primitive.

[a] This parameter is for further study.

The primitive "N-DATA ACKNOWLEDGE" is used when the delivery confirmation service is selected. This primitive is for further study.

The primitive N-RESET (Table 5/Q.711) can occur in the data transfer state of a connection with a protocol class including flow control. N-RESET overrides all other activities and causes the SCCP to start a re-initialization procedure for sequence numbering. N-RESET appears as a request, an indication, a response and a confirmation. After reception of a N-RESET request and before the sending of a N-RESET confirmation, all NSDUs from SCCP are discarded by th SCCP.

TABLE 5/Q.711

**Parameters of the primitive N-RESET**

| Parameter | Primitive | | | |
|---|---|---|---|---|
| | N-RESET request | N-RESET indication | N-RESET response | N-RESET confirmation |
| Originator | | X | | |
| Reason | X | X | | |
| Connection identification [a)] | X | X | X | X |

X Parameter present within the primitive.

[a)] This parameter is for further study.

The parameter "Originator" indicates the source of the reset and can be any of the following: the "network service provider" (network originated), the "network service user" (user originated), or "undefined". The parameter "Reason" indicates "network service provider congestion", "reason unspecified" or "local SCCP originated" for a network originated reset, and indicates "user synchronization" for a user originated reset. The "Reason" parameter is "undefined" when the "Originator" parameter is "undefined".

2.1.1.2.4 *Release phase*

The primitives for the release phase are N-DISCONNECT request and N-DISCONNECT indication. These primitives are also used for the connection refusal during connection establishment phase. Parameters are included to notify the reason for connection release/refusal and the initiator of the connection release/refusal procedure. User data may be also be included (see Table 6/Q.711).

The parameter "Originator" indicates the initiator of the connection release or the connection refusal. It may assume the following values:

- the network service provider,
- the network service user,
- undefined.

TABLE 6/Q.711

**Parameters of the primitive N-DISCONNECT**

| Parameter | Primitive | |
|---|---|---|
| | N-DISCONNECT request | N-DISCONNECT indication |
| Originator | | X |
| Responding address | X | X |
| Reason | X | X |
| User data | X | X |
| Connection identification [a] | X | X |

X Parameter present within the primitive.

[a] This parameter is for further study.

The parameter "Reason" gives information about the cause of the connection release or the connection refusal. It may assume any of the following values in accordance with the value of the "Originator":

1) When the "Originator" parameter indicates the "network service provider":
   - disconnection – abnormal condition of non-transient nature;
   - disconnection – abnormal condition of transient nature;
   - disconnection – invalid state [1];
   - disconnection – release in progress [1];
   - connection refusal [2] – destination address unknown (non-transient condition) [1];
   - connection refusal [2] – destination inaccessible/non-transient condition [1];
   - connection refusal [2] – destination inaccessible/transient condition [1];
   - connection refusal [2] – QOS not available/non-transient condition [1];
   - connection refusal [2] – QOS not available/transient condition [1];
   - connection refusal [2] – reason unspecified/non-transient condition [1];
   - connection refusal [2] – reason unspecified/transient condition [1];
   - connection refusal [2] – local error [1];
   - connection refusal [2] – invalid state [1];
   - connection refusal [2] – no translation [1];
   - connection refusal [2] – in restart phase [1].

[1] These values may be used locally at the originating/initiating node as an implementation option.

[2] It is noted that the term "connection rejection" is used in Recommendation X.213 for the "Reason" parameter values.

2) When the "Originator" parameter indicates the "network service user":
   - disconnection – normal condition;
   - disconnection – abnormal condition;
   - disconnection – end user congestion;
   - disconnection – end user failure;
   - disconnection – SCCP user originated;
   - disconnection – access congestion;
   - disconnection – access failure;
   - disconnection – subsystem congestion;
   - connection refusal[3] – non-transient condition;
   - connection refusal[3] – transient condition;
   - connection refusal[3] – incompatible information in NSDUs;
   - connection refusal[3] – end user originated;
   - connection refusal[3] – end user congestion;
   - connection refusal[3] – end user failure;
   - connection refusal[3] – SCCP user originated;
   - connection refusal[3] – access congestion;
   - connection refusal[3] – access failure;
   - connection refusal[3] – subsystem congestion.

3) When the "Originator" parameter is "undefined", then the "Reason" parameter is also "undefined".

*Note* – Addition to, or refinement of, this list of possible values for the parameter "Reason" to convey more specific diagnostic, cause and management information is for further study.

2.1.1.3 *Additional SCCP primitive and interface elements*

In addition to those primitives in Recommendation X.213, there is a primitive N-INFORM needed by the SCCP connection-oriented services during data transfer phase. There are also three interface elements used by User Part Type A, e.g. ISDN-UP, as in Figure 1/Q.711.

2.1.1.3.1 *Notice service*

The provision of the notice service by use of the "N-INFORM" primitive is for further study.

The primitive N-INFORM (Table 7/Q.711) is used during data transfer to convey relevant network/user information. The primitive "N-INFORM" will contain the parameters "Reason', "Connection Identification" and "QOS parameter set".

The primitive "N-INFORM request" is provided to inform the SCCP of the connection user failure/congestion, or anticipated QOS changes. A further primitive "N-INFORM indication" is provided to indicate actual failures of the SCCP to the SCCP-user functions or anticipated quality of service changes or other indications to the SCCP-user functions.

The parameter "Reason" contains the network/user information to be conveyed. It may assume the following values:

- network service provider failure;
- network service congestion;
- network service provider QOS change;
- network service user failure;
- network service user congestion;
- network service user QOS change;
- reason unspecified.

[3] It is noted that the term "connection rejection" is used in Recommendation X.213 for the "Reason" parameter values.

TABLE 7/Q.711

**Parameters of the primitive N-INFORM**

| Parameter | Primitive | |
|---|---|---|
| | N-INFORM request | N-INFORM indication |
| Reason | X | X |
| Connection identification [a)] | X | X |
| QOS parameter set [a)] | X | X |

X Parameter present within the primitive.

[a)] Parameter is for further study.

2.1.1.3.2 *Connection establishment interface elements*

For the User Part Type A in Figure 1/Q.711, two mechanisms are available to set up a signalling connection. For example, the ISDN-User Part may use the mechanism described in § 2.1.1.2.2 or may request the SCCP to initiate a connection and return the information to the ISDN-User Part for transmission within an ISDN-User-Part call setup message, like an Initial Address Message (IAM).

Three interface elements are defined for the information flow between SCCP and ISDN-User Part:

a) REQUEST to the SCCP, Type 1 and Type 2;

b) REPLY from the SCCP.

The REQUEST Type 1 contains the following parameters:

- connection identification (for further study);
- receipt confirmation selection;
- expedited data selection;
- quality of service parameter set.

The REQUEST Type 2 contains the following parameters:

- protocol class;
- credit;
- connection identification (for further study);
- source local reference;
- originating signalling point code;
- reply request;
- refusal indicator.

The REPLY contains the following parameters:

- source local reference;
- protocol class;
- credit;
- connection identification (for further study).

2.1.2 *Permanent signalling connections*

2.1.2.1 *Description*

The setup/release service is controlled by the Administration (e.g. O&M application). The functions for setup and release may be similar to those provided for temporary signalling connections and are for further study. The classes of service are the same.

Permanently established signalling connections may require additional safeguarding mechanisms within the endpoints (relaypoints) of the connection in order to guarantee their re-establishment in case of a processor outage followed by a recovery.

2.1.2.2 *Primitives and parameters*

The primitives and their parameters are listed in Table 8/Q.711. Their content and functionality correspond to the description within § 2.1.1.2.3.

TABLE 8/Q.711

**Primitives for the data transfer on permanent connections**

| Primitives | | Parameters |
|---|---|---|
| Generic Name | Specific Name | |
| N-DATA | Request<br>Indication | Confirmation request<br>User data<br>Connection identification [a] |
| N-EXPEDITED DATA | Request<br>Indication | User data<br>Connection identification [a] |
| N-DATA ACKNOWLEDGE<br>(for further study) | Request<br>Indication | Connection identification [a] |
| N-RESET | Request<br>Indication<br>Response<br>Confirmation | Originator<br>Reason<br>Connection identification [a] |

[a] Parameter is for further study.

2.2 *Connectionless services*

The SCCP provides the SCCP user with the ability to transfer signalling messages via the signalling network without setup of a signalling connection. In addition to the MTP capability, a "Routing" function has to be provided within the SCCP, which maps the called address to the Signalling Point Codes of the MTP Service.

This mapping function may be provided within each node or might be distributed over the network or could be provided in some special translation centres.

Under certain conditions of congestion and unavailability of subsystems and/or signalling points, connectionless messages could be discarded instead of being delivered. If the SCCP user wishes to be informed of the non-delivery of messages, the Return Option parameter must be set to "return message on error" in the primitive to the SCCP.

2.2.1 *Description*

There are two possibilities to transfer data without a connection setup with regard to the sequence control mechanisms provided by the MTP.

a) The MTP guarantees (to a high degree of probability) an in-sequence delivery of messages which contain the same Signalling Link Selection (SLS) code. The SCCP user can demand this MTP service by allocating a parameter "Sequence control" into the primitive to the SCCP. The SCCP will put the same SLS code into the primitive to the MTP for all primitives from the SCCP user with the same "Sequence control" parameter.

b) If the in-sequence delivery is not required, the SCCP can insert SLS codes randomly or with respect to appropriate load sharing within the signalling network.

The rules to achieve load sharing are not defined in the SCCP Recommendations.

2.2.2 *Primitives and parameters of the connectionless service*

2.2.2.1 *Overview*

Table 9/Q.711 gives an overview of the primitives to the upper layers and the corresponding parameters for the connectionless service.

TABLE 9/Q.711

**Primitives and parameters of the connectionless service**

| Primitives | | Parameters |
|---|---|---|
| Generic Name | Specific Name | |
| N-UNITDATA | Request<br>Indication | Called address<br>Calling address<br>Sequence control [a]<br>Return option [a]<br>User data |
| N-NOTICE | Indication | Called address<br>Calling address<br>Reason for return<br>User data |

[a] An integration of the parameter Sequence control/Return option into the Quality of Service parameter set is for further study.

2.2.2.2 *Parameters*

2.2.2.2.1 *Address*

The parameters "Called address" and "Calling address" serve to identify the destination and origination respectively, of the connectionless message. These parameters may contain some combination of global titles, subsystem numbers, and signalling point codes.

2.2.2.2.2 *Sequence control*

The parameter "Sequence control" indicates to the SCCP whether the user wishes the service "sequence guaranteed" or the service "sequence not guaranteed". In the case of "sequence guaranteed" service, this parameter is an indication to the SCCP that a given stream of messages with the same called address has to be delivered in sequence by making use of the features of the MTP. In addition, this parameter is also used to distinguish different streams of messages so that the SCCP can allocate SLS codes appropriately to help the MTP in achieving an even distribution of signalling traffic.

2.2.2.2.3 *Return option*

The parameter "Return option" is used to determine the handling of messages encountering transport problems.

"Return option" may assume the following values:

- discard message on error;
- return message on error.

2.2.2.2.4 *Reason for return*

The parameter "Reason for return" identifies the reason why a message was not able to be delivered to its final destination.

"Reason for return" may assume the following values:

- no translation for an address of such nature;
- no translation for this specific address;
- subsystem configuration;
- subsystem failure;
- unequipped user;
- network congestion;
- network failure.

2.2.2.2.5 *User data*

The parameter "User data" is information which is to be transferred transparently between SCCP users.

2.2.2.3 *Primitives*

2.2.2.3.1 *UNITDATA*

The "N-UNITDATA request" primitive is the means by which a SCCP user requests the SCCP to transport data to another user.

The "N-UNITDATA indication" primitive informs a user that data is being delivered to it from the SCCP.

Table 10/Q.711 indicates the parameters of the primitive N-UNITDATA.

2.2.2.3.2 *NOTICE*

The "N-NOTICE indication" primitive is the means by which the SCCP returns to the originating user a message which could not reach the final destination.

Table 11/Q.711 indicates the parameters of the primitive N-NOTICE.

TABLE 10/Q.711

**Parameters of the primitive N-UNITDATA**

| Parameter | Primitive | |
|---|---|---|
| | N-UNITDATA request | N-UNITDATA indication |
| Called address | X | X |
| Calling address | X | X |
| Sequence control [a] | X | |
| Return option | X | |
| User data | X | X |

[a] The inclusion of this parameter in the N-UNITDATA indication primitive is for further study.

TABLE 11/Q.711

**Parameters of the primitive N-NOTICE**

| Parameter | Primitive |
|---|---|
| | N-NOTICE indication |
| Called address | X |
| Calling address | X |
| Reason for return | X |
| User data | X |

## 2.3 *SCCP management*

### 2.3.1 *Description*

The SCCP provides SCCP management procedures (see Recommendation Q.714, § 5) to maintain network performances by rerouting or throttling traffic in the event of failure or congestion in the network. These SCCP management procedures apply to both the connection-oriented and the connectionless services of the SCCP.

### 2.3.2 *Primitives and parameters of the SCCP management*

#### 2.3.2.1 *Overview*

Table 12/Q.711 gives an overview of the primitives to the upper layers and the corresponding parameters for the SCCP management.

TABLE 12/Q.711

**Primitives and parameters of the SCCP management**

| Primitives | | Parameters |
|---|---|---|
| Generic Name | Specific Name | |
| R-COORD | Request<br>Indication<br>Response<br>Confirmation | Affected subsystem<br>Subsystem multiplicity indicator |
| N-STATE | Request<br>Indication | Affected subsystem<br>User status<br>Subsystem multiplicity indicator |
| N-PCSTATE | Indication | Affected DPC<br>*Signalling Point Status* |

#### 2.3.2.2 *Parameters*

##### 2.3.2.2.1 *Address*

See § 2.2.2.2.1.

##### 2.3.2.2.2 *Affected subsystem*

The parameter "Affected subsystem" identifies a user which is failed, withdrawn, congested, or allowed. The "Affected subsystem" parameter contains the same type of information as the "Called address" and "Calling address".

##### 2.3.2.2.3 *User status*

The parameter "User status" is used to inform a SCCP user of the status of the affected subsystem.

"User status" may assume one of the following values:

- User-in-service (UIS);
- User-out-of-service (UOS).

2.3.2.2.4 *Subsystem multiplicity indicator*

The parameter "Subsystem multiplicity indicator" identifies the number of replications of a subsystem.

2.3.2.2.5 *Affected DPC*

The parameter "Affected DPC" identifies a signalling point which is failed, congested, or allowed. The "Affected DPC" parameter contains unique identification of a signalling point.

2.3.2.2.6 *Signalling point status*

The parameter "Signalling point status" is used to inform a user of the status of an affected DPC.

"Signalling point status" may assume the following values:

- Signalling point inaccessible,
- Signalling point congested,
- Signalling point accessible.

2.3.2.3 *Primitives*

2.3.2.3.1 *COORD*

The "N-COORD" primitive (Table 13/Q.711) is used by replicated subsystems to coordinate the withdrawal of one of the subsystems.

The primitive exists as: a "request" when the originating user is requesting permission to go out of service; an "indication" when the request to go out of service is delivered to the originator's replicate; a "response" when the originator's replicate announced it has sufficient resources to let the originator go out of service; and as a "confirmation" when the originator is informed that it may go out of service.

TABLE 13/Q.711

**Parameters of the primitive N-COORD**

| Parameter | Primitive | | | |
|---|---|---|---|---|
| | N-COORD request | N-COORD indication | N-COORD response | N-COORD confirmation |
| Affected subsystem | X | X | X | X |
| Subsystem multiplicity indicator | | X | | X |

2.3.2.3.2 *STATE*

The "N-STATE request" primitive (Table 14/Q.711) is used to inform the SCCP management about the status of the originating user. The "N-STATE indication" primitive is used to inform an SCCP user accordingly.

TABLE 14/Q.711

**Parameters of the primitive N-STATE**

| Parameter | Primitive | |
|---|---|---|
| | N-STATE request | N-STATE indication |
| Affected subsystem | X | X |
| User status | X | X |
| Subsystem multiplicity indicator | | X |

2.3.2.3.3 *PCSTATE*

The "N-PCSTATE primitive" (Table 15/Q.711) is used to inform a user about the status of a signalling point.

TABLE 15/Q.711

**Parameters of the primitive N-PCSTATE**

| Parameter | Primitive |
|---|---|
| | N-PCSTATE indication |
| Affectedd DPC | X |
| Signalling Point Status | X |

## 3 Services assumed from the MTP

### 3.1 *Description*

This paragraph describes the functional interface offered by the MTP to the upper layer functions, i.e., the SCCP and the User Parts. In order to align the terminology with the OSI-Model, the description uses the terms "primitives" and "parameters".

## 3.2 *Primitives and parameters*

The primitives and parameters are shown in Table 16/Q.711.

TABLE 16/Q.711

**Message transfer part service primitives**

| Primitives | | Parameters |
|---|---|---|
| Generic Name | Specific Name | |
| MTP-TRANSFER | Request<br>Indication | OPC<br>DPC<br>SLS<br>SIO<br>User Data |
| MTP-PAUSE<br>(Stop) | Indication | Affected DPC |
| MTP-RESUME<br>(Start) | Indication | Affected DPC |
| MTP-STATUS | Indication | Affected DPC<br>Cause [a] |

[a] The cause parameter has, at present, two values:

i) *Signalling network congested (level)*

This level value is applicable if national option with congestion priorities and multiple signalling link states without congestion priorities as in Recommendation Q.704 is implemented.

ii) *Remote user unavailable.*

### 3.2.1 *TRANSFER*

The primitive "MTP-TRANSFER" is used between level 4 and level 3 (SMH) to provide the MTP message transfer service.

### 3.2.2 *PAUSE*

The primitive "MTP-PAUSE" indicates to the SCCP total inability of providing the MTP service to the specified destination.

This primitive corresponds to the destination inaccessible state as defined in Recommendation Q.704.

3.2.3 *RESUME*

The primitive "MTP-RESUME" indicates to the SCCP total ability of providing the MTP service to the specified destination.

This primitive corresponds to the destination accessible state as defined in Recommendation Q.704.

3.2.4 *STATUS*

The primitive "MTP-STATUS" indicates to the SCCP partial inability of providing the MTP service to the specified destination, or the unavailability of the remote peer user. The response of the SCCP for the latter case is for further study.

In the case of national option with congestion priorities and multiple signalling link congestion states without priorities as in Recommendation Q.704 is implemented, this "MTP-STATUS" primitive is also used to indicate a change of congestion level.

This primitive corresponds to the destination congested state as defined in Recommendation Q.704.

## 4 Functions provided by the SCCP

This section is an overview of the functional blocks within the SCCP.

### 4.1 *Connection-oriented functions*

#### 4.1.1 *Functions for temporary signalling connections*

##### 4.1.1.1 *Connection establishment functions*

The connection establishment service primitives defined in § 2 are used to set up a signalling connection.

The main functions of the connection establishment phase are listed below:

- Setup of a signalling connection;
- Establish the optimum size of NPDUs (Network Protocol Data Unit);
- Map network address onto signalling relations;
- Select functions operational during data transfer phase (for instance, layer service selection);
- Provide means to distinguish network connections;
- Transport user data (within the request).

##### 4.1.1.2 *Data transfer phase function*

The data transfer phase functions provide means for a two-way simultaneous transport of messages between the two endpoints of the signalling connection.

The main functions of the data transfer phase as listed below are used or not used in accordance with the result of the selection performed in the connection establishment phase.

- Segmenting/reassembling,
- Flow control,
- Connection identification,
- NSDU delimiting (M-Bit),
- Expedited data,
- Missequence detection,
- Reset,
- Receipt confirmation [4],
- Others.

[4] The need for this functions is for further study.

4.1.1.3 *Release phase functions*

These functions provide disconnection of the signalling connection, regardless of the current phase of the connection. The release may be performed by an upper layer stimulus or by maintenance of the SCCP itself. The release can start at each end of the connection (symmetrical procedure).

The main function of the release phase is the disconnection.

4.1.2 *Functions for permanent signalling connections*

4.1.2.1 *Connection establishment phase and connection release phase functions*

The setup and release for permanent signalling connections are for further study. The stimuli for setup and release of permanent connections are originated from the Administration function.

4.1.2.2 *Data transfer phase functions*

The functions for the data transfer on permanent signalling connections correspond to that for temporary connections. Differences may exist regarding the quality of service. This matter is for further study.

4.2 *Connectionless service functions*

The functions of the connectionless service are listed below:

- mapping the network address to signalling relations,
- sequence service classification.

4.3 *Management functions* (for further study)

The SCCP provides functions which manage the status of the SCCP subsystems. These functions allow other nodes in the network to be informed of the change in status of SCCP subsystems at a node, and to modify SCCP translation data if appropriate. Subsystem congestion management is for further study.

Functions are also provided to allow a coordinated change of status of replicated SCCP subsystems. At present, this allows a replicated subsystem to be withdrawn from service.

When a subsystem is out of service, SCCP test functions are activated at nodes receiving unavailability information. At periodic intervals the status of the unavailable subsystem is checked by a SCCP management procedure.

Broadcast functions within SCCP management broadcast subsystem status changes to nodes within the network which have an immediate need to be informed of a particular signalling point/subsystem status change.

Notification functions to local subsystems within the node (local broadcast) are also provided.

4.4 *Routing and translation functions* (for further study)

The SCCP routing provides a powerful address translation function, which is asked for connectionless and connection-oriented service. Detailed description of the SCCP routing function can be found in Recommendation Q.714, §§ 2.2 and 2.3.

The basic translation function performed by the SCCP is to transfer the SCCP address parameter from a global title to a point code and a subsystem number. Other translation results are also possible. The global title form of the address could typically be dialed digits (e.g. a Freephone (800) number). Several standardized CCITT numbering plans may be supported by SCCP; details are given in Recommendation Q.713, § 3.4.

The address translation capabilities of the SCCP in relation to handling OSI Network Service Access Points (NSAP) are for further study.

ANNEX A

(to Recommendation Q.711)

**OSI network layer conformance**

The following information should be taken into account when reading Recommendation Q.711 in relation to the provision of an OSI network layer service.

All references to connectionless classes 0 and 1 are not included in Recommendation X.200.

*§ 2.1.1*

The Connection identification parameters in the following primitives are implicit in Recommendation X.213:

N-CONNECT

N-DATA

N-EXPEDITED DATA

N-DATA ACKNOWLEDGE

N-DISCONNECT

N-RESET

The N-INFORM primitive does not exist within Recommendation X.213.

The connection establishment interface elements described in § 2.1.1.3.2 is not required to support an OSI network layer service.

*§ 2.1.2*

Permanent connection services are not defined in Recommendation X.200 and are not required to support an OSI network layer service. The service is offered by the SCCP for specific No. 7 applications.

*§ 2.2*

Connectionless network service is still under study in Study Group VII and is not defined in Recommendation X.213.

*§ 2.3*

This section on SCCP management is not defined in Recommendation X.213 and none of the primitives exist in OSI.

APPENDIX

(to Recommendation Q.711)

**Unresolved issues in SCCP Recommendations**

This appendix lists the topics in SCCP on which study is continuing in the next study period. It is not an exhaustive list, but does indicate where the Recommendations might change. In these areas, RPOAs may need to supplement the Recommendations, but in such a way as not to conflict with ongoing work; implementors should consider likely future developments and, where possible, design to accommodate these.

The topics under study are listed below; the references are to the Blue Book.

1) Inter-nodal communication model with SCCP connectionless service (§ 1.3.3, Rec. Q.711);

2) Delivery confirmation service (N-DATA ACKNOWLEDGE primitive) (Table 1/Q.711);

3) Transitions caused by N-DATA ACK primitive (Figure 7/Q.711);

4) Facilities causing differences in the called and responding addresses in N-CONNECT request and response (§ 2.1.1.2.2, Rec. Q.711);

5) The need for Receipt Confirmation Service in SCCP (§§ 2.1.1.2.2 and 4.1.1.2, Rec. Q.711);

6) Connection identification parameter inclusion in Request types 1 and 2, and reply primitives between SCCP and ISUP (§ 2.1.1.3.2, Rec. Q.711);

7) Connection identification parameter inclusion in N-CONNECT, N-DATA, N-EXPEDITED DATA, N-RESET, and N-DISCONNECT primitives (Tables 2/Q.711, 3/Q.711, 4/Q.711, 5/Q.711, 6/Q.711, 7/Q.711, 8/Q.711);

8) The list of release reason parameter values (§ 2.1.1.2, Rec. Q.711);

9) QOS parameter set inclusion in N-INFORM (Table 7/Q.711);

10) Setup and release functions for permanent signalling connections (§ 2.1.2.1, Rec. Q.711);

11) Integrating sequence control and return option parameters in the QOS set (Table 9/Q.711);

12) Sequence control parameter inclusion in the N-UNITDATA indication primitive (Table 10/Q.711);

13) SCCP response to MTP-STATUS (§ 3.2.4, Rec. Q.711);

14) Difference in QOS between permanent and temporary signalling connections (§ 4.1.2.2, Rec. Q.711);

15) SCCP management procedures for subsystem congestion (§ 4.3, Rec. Q.711; §§ 3.11, 3.12, 3.15, Rec. Q.713; §§ 5.1, 5.3, Rec. Q.714);

16) SCCP capabilities in OSI NSAP address translation (§ 4.4, Rec. Q.711);

17) Possible need for diagnostic parameter (§ 2.6, Rec. Q.712);

18) Constraints on order of optional parameter transmission (§ 1.8, Rec. Q.713);

19) Destination local reference coded as all ones (§ 3.2, Rec. Q.713);

20) Source local reference coded as all ones (§ 3.3, Rec. Q.713);

21) Alignment with X.96 call progress information (§§ 3.11, 3.15, Rec. Q.713);

22) Inclusion of routing failure causes as for return cause in Recommendation Q.713, § 3.12 (§ 3.15, Rec. Q.713);

23) Data parameter maximum length for *Unitdata* and *Unitdata Service* messages (§§ 4.10, 4.11, Rec. Q.713; §§ 1.1.2, 4, Rec. Q.714);

24) Need for *Released message* cause value 1110 "not obtainable" (Annex A, Rec. Q.713);

25) Need for *Reset Request* message cause value 1011 "not obtainable" (Annex A, Rec. Q.713);

26) Notification regarding unrecognized messages/parameters (§ 1.14, Rec. Q.714);

27) Classification of SCCP routing failure causes (§ 2.4, Rec. Q.714);

28) Management procedures for non-dominant mode nodes/subsystems with more than one backup (§ 5.1, Rec. Q.714);

29) Receipt from a local originating subsystem of a message for a prohibited subsystem (§ 5.3.2.1, Rec. Q.714);

30) Possible introduction of a subsystem out of service denial message (§ 5.3.5.3, Rec. Q.711);

31) Mathematical analysis of SCCP performance;

32) Recommendation Q.716 parameter valus (§ 3, Rec. Q.716).

**Recommendation Q.712**

## DEFINITION AND FUNCTION OF SCCP MESSAGES

### 1 Signalling connection control part messages

The signalling connection control part (SCCP) messages are used by the peer-to-peer protocol. All messages are uniquely identified by means of a message type code, which is to be found in all the messages. The meaning and definition of the various parameter fields contained in these messages are specified in § 2. The actual inclusion of these parameter fields in a given message depends on the class of protocol and is specified in § 3.

#### 1.1 Connection Confirm (CC)

A *Connection Confirm* message is sent by the called SCCP to indicate to the calling SCCP that it has performed the setup of the signalling connection. On reception of a *Connection Confirm* message, the calling SCCP completes the setup of the signalling connection, if possible.

It is used during connection establishment phase by connection-oriented protocol class 2 or 3.

#### 1.2 Connection Request (CR)

A *Connection Request* message is sent by a calling SCCP to a called SCCP to request the setting up of a signalling connection between the two entities. The required characteristics of the signalling connection are carried in various parameter fields. On reception of a *Connection Request* message, the called SCCP initiates the setup of the signalling connection if possible.

It is used during connection establishment phase by connection-oriented protocol class 2 or 3.

#### 1.3 Connection Refused (CREF)

A *Connection Refused* message is sent by the called SCCP or an intermediate node SCCP to indicate to the calling SCCP that the setup of the signalling connection has been refused.

It is used during connection establishment phase by connection-oriented protocol class 2 or 3.

#### 1.4 Data Acknowledgement (AK)

A *Data Acknowledgement* message is used to control the window flow control mechanism, which has been selected for the data transfer phase.

It is used during the data transfer phase in protocol class 3.

#### 1.5 Data Form 1 (DT1)

A *Data Form 1* message is sent by either end of a signalling connection to pass transparently SCCP user data between two SCCP nodes.

It is used during the data transfer phase in protocol class 2 only.

#### 1.6 Data Form 2 (DT2)

A *Data Form 2* message is sent by either end of a signalling connection to pass transparently SCCP user data between two SCCP nodes and to acknowledge messages flowing in the other direction.

It is used during the data transfer phase in protocol class 3 only.

### 1.7 Expedited Data (ED)

An *Expedited Data* message functions as a *Data Form 2* message but includes the ability to bypass the flow control mechanism which has been selected for the data transfer phase. It may be sent by either end of the signalling connection.

It is used during the data transfer phase in protocol class 3 only.

### 1.8 Expedited Data Acknowledgement (EA)

An *Expedited Data Acknowledgement* message is used to acknowledge an *Expedited Data* message. Every ED message has to be acknowledged by an EA message before another ED message may be sent.

It is used during the data transfer phase in protocol class 3 only.

### 1.9 Inactivity Test (IT)

An *Inactivity Test* message may be sent periodically by either end of a signalling connection to check if this signalling connection is active at both ends, and to audit the consistency of connection data at both ends.

It is used in protocol classes 2 and 3.

### 1.10 Protocol Data Unit Error (ERR)

A *Protocol Data Unit Error* message is sent on detection of any protocol errors.

It is used during the data transfer phase in protocol classes 2 and 3.

### 1.11 Released (RLSD)

A *Released* message is sent, in the forward or backward direction, to indicate that the sending SCCP wants to release a signalling connection and the associated resources at the sending SCCP have been brought into the disconnect pending condition. It also indicates that the receiving node should release the connection and any other associated resources as well.

It is used during connection release phase in protocol classes 2 and 3.

### 1.12 Release Complete (RLC)

A *Release Complete* message is sent in response to the *Released* message indicating that the *Released* message has been received, and the appropriate procedures has been completed.

It is used during connection release phase in protocol classes 2 and 3.

### 1.13 Reset Confirm (RSC)

A *Reset Confirm* message is sent in response to a *Reset Request* message to indicate that *Reset Request* has been received and the appropriate procedure has been completed.

It is used during the data transfer phase in protocol class 3.

### 1.14 Reset Request (RSR)

A *Reset Request* message is sent to indicate that the sending SCCP wants to initiate a reset procedure (re-initialization of sequence numbers) with the receiving SCCP.

It is used during the data transfer phase in protocol class 3.

### 1.15 Subsystem-Allowed (SSA)

A *Subsystem-Allowed* message is sent to concerned destinations to inform those destinations that a subsystem which was formerly prohibited is now allowed.

It is used for SCCP subsystem management.

### 1.16 Subsystem-Out-of-Service-Grant (SOG)

A *Subsystem-Out-of-Service-Grant* message is sent, in response to a *Subsystem-Out-of-Service-Request* message, to the requesting SCCP if both the requested SCCP and the backup of the affected subsystem agree to the request.

It is used for SCCP subsystem management.

### 1.17 Subsystem-Out-of-Service-Request (SOR)

A *Subsystem-Out-of-Service* message is used to allow subsystems to go out-of-service without degrading performance of the network. When a subsystem wishes to go out-of-service, the request is transferred by means of a *Subsystem-Out-of-Service-Request* message between the SCCP at the subsystem's node and the SCCP at the duplicate subsystem's node.

It is used for SCCP subsystem management.

### 1.18 Subsystem-Prohibited (SSP)

A *Subsystem-Prohibited* message is sent to concerned destinations to inform SCCP Management (SCMG) at those destinations of the failure of a subsystem.

It is used for SCCP subsystem management.

### 1.19 Subsystem-Status-Test (SST)

A *Subsystem-Status-Test* message is sent to verify the status of a subsystem marked prohibited.

It is used for SCCP subsystem management.

### 1.20 Unitdata (UDT)

A *Unitdata* message is used by a SCCP wanting to send data in a connectionless mode.

It is used in connectionless protocol classes 0 and 1.

### 1.21 Unitdata Service (UDTS)

A *Unitdata Service* message is used to indicate to the originating SCCP that a UDT it sent cannot be delivered to its destination. A UDTS message is sent only when the option field in that UDT is set to "return on error".

It is used in connectionless protocol classes 0 and 1.

## 2 SCCP parameter

### 2.1 affected point code

The "affected point code" identifies a signalling point where the affected subsystem is located.

### 2.2 affected subsystem number

The "affected subystem number" parameter field identifies a subsystem which is failed, withdrawn, congested or allowed. In the case of SST messages, it also identifies the subsystem being audited. In the case of SOR or SOG messages, it identifies a subsystem requesting to go out of service.

### 2.3 calling/called party address

The "calling/called party address" parameter field contains enough information to uniquely identify the origination/destination signalling point and/or the SCCP service access point.

It can be any combination of a global title (dialled digits for example), a signalling point code, and a subsystem number. The subsystem number (SSN) identifies a SCCP user function when provided.

In order to allow the interpretation of this address, it begins with an address indicator indicating which information elements are present. The address indicator also includes a routing indicator specifying if translation is required, and a global title indicator specifying global title format.

The "calling/called party address" parameter field has two different meanings depending on whether it is included in a connection-oriented or connectionless message.

For a connection-oriented message, the significance of these fields is related to the direction of the connection setup (i.e. independent of the direction the message is going.

For a connectionless message, the significance of these fields is dependent on the direction the message is going (just as for OPC and DPC).

### 2.4 credit

The "credit" parameter field is used in the acknowledgements to indicate to the sender how many messages it may send, i.e., window size. It is also used in the CR and CC message to indicate the proposed and selected credit, and in the IT message to audit the consistency of this connection data at both ends of a connection section.

### 2.5 data

The "data" parameter field contains information coming from upper layers or from SCCP management.

In connectionless and connection-oriented messages the data parameter field contains information coming from the upper layers.

Information coming from SCCP management will be contained in the data parameter field of a UDT message. In this case the data parameter field of the UDP message will only contain the SCCP management message.

### 2.6 diagnostic

The "diagnostic" parameter field is for further study.

### 2.7 error cause

The "error cause" parameter field is used in the *Protocol Data Unit Error* message in order to indicate what is the exact protocol error.

### 2.8 end of optional parameters

The "end of optional parameters" parameter field is used in any message containing optional parameters to indicate where the part allocated to these optional parameters ends.

### 2.9 local reference number (source/destination)

The "local reference number (source/destination)" parameter field uniquely identifies in a node a signalling connection. It is an internal working number chosen by each node independently from the destination node. At least one local reference number is to be found in any message exchanged on a signalling connection section.

*Note* – Remote reference number is used to reflect the local reference number at the remote end of a connection section.

### 2.10 protocol class

For connection-oriented protocol classes, the "protocol class" parameter field is used during the connection establishment phase; it is negotiated between the two end SCCP. It is also used during data transfer phase to audit the consistency of this connection data at both ends of a connection section.

For connectionless protocol classes the "protocol class" parameter field is used to indicate whether or not a message should be returned on error occurence.

2.11 **receive sequence number**

The "receive sequence number" parameter field P(R) is used in the data acknowledgement message to indicate the lower edge of the receiving window.

It also indicates that at least all messages numbered up to and including P(R) – 1 are accepted.

2.12 **refusal cause**

The "refusal cause" parameter field is used in a *Connection Refused* message to indicate the reason why the connection setup request was refused.

2.13 **release cause**

The "release cause" parameter field is used in a *Released* message to indicate the reason of the release.

2.14 **reset cause**

The "reset cause" parameter field is used in a *Reset Request* message to indicate the reason why a reset procedure is invoked.

2.15 **return cause**

For connectionless protocol classes, the "return cause" parameter field is used to indicate the reason why a message was returned.

2.16 **segmenting/reassembling**

The "segmenting/reassembling" parameter field is used in the data message for the segmenting and reassembling function. It is the more data indicator (M-bit). This is used only in connection-oriented messages.

It is set to one in a data message to indicate that more data will follow in a subsequent message.

It is set to zero in a data message to indicate that the data in this message forms the end of a complete data sequence.

2.17 **sequencing/segmenting**

The "sequencing/segmenting" parameter field contains the information necessary for the following functions: sequence numbering, flow control, segmenting and reassembling.

2.18 **subsystem multiplicity indicator**

The "subsystem multiplicity indicator" is used in SCCP management messages to indicate the number of associated replicated subsystems.

## 3 Inclusion of fields in the messages

The inclusion of the information elements specified in § 2 in the various messages specified in § 1 according to their type depends on the class of protocol. SCCP messages are specified in Table 1/Q.712 and SCCP management messages are specified in Table 2/Q.712.

All SCCP management messages are embedded in the "data" parameter of the *Unitdata* message.

The following applies to Tables 1/Q.712 and 2/Q.712:

m mandatory field

o optional field (which is included in a message when needed)

TABLE 1/Q.712

**Inclusion of fields in messages**

| Parameter field \ Messages | CR | CC | CREF | RLSD | RLC | DT1 | DT2 | AK | ED | EA | RSR | RSC | ERR | IT | UDT | UDTS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Destination local reference number | | m | m | m | m | m | m | m | m | m | m | m | m | m | | |
| Source local reference number | m | m | | m | m | | | | | | m | m | | m | | |
| Called party address | m | o | o | | | | | | | | | | | | m | m |
| Calling party address | o | | | | | | | | | | | | | | m | m |
| Protocol class | m | m | | | | | | | | | | | | m | m | |
| Segmenting/Reassembling | | | | | | m | | | | | | | | | | |
| Receive sequence number | | | | | | | | m | | | | | | | | |
| Sequencing/Segmenting | | | | | | | m | | | | | | | m [a)] | | |
| Credit | o | o | | | | | | m | | | | | | m [a)] | | |
| Release cause | | | | m | | | | | | | | | | | | |
| Return cause | | | | | | | | | | | | | | | | m |
| Reset cause | | | | | | | | | | | m | | | | | |
| Error cause | | | | | | | | | | | | | m | | | |
| User data | o | o | o | o | | m | m | | m | | | | | | m | m |
| Refusal cause | | | m | | | | | | | | | | | | | |
| End of optional parameters | o | o | o | o | | | | | | | | | | | | |

[a)] Information in these parameter fields are ignored if the protocol class parameter indicates class 2.

TABLE 2/Q.712

**SCCP management messages**

| Parameter fields \ Messages | SSA | SSP | SST | SOR | SOG |
|---|---|---|---|---|---|
| SCMG format ID | m | m | m | m | m |
| Affected SSN | m | m | m | m | m |
| Affected PC | m | m | m | m | m |
| Subsystem multiplicity indicator | m | m | m | m | m |

**Recommendation Q.713**

## SCCP FORMATS AND CODES

### 1 General

The Signalling Connection Control Part (SCCP) messages are carried on the signalling data link by means of Signal Units the format of which is described in Recommendation Q.703, § 2.2.

The Service Information Octet format and coding is described in Recommendation Q.704, § 14.2. The Service Indicator is coded 0011 for the SCCP.

The Signalling Information Field (SIF) of each Message Signal Unit containing an SCCP message consists of an integral number of octets.

A message consists of the following parts (see Figure 1/Q.713):

- the routing label;
- the message type code;
- the mandatory fixed part;
- the mandatory variable part;
- the optional part, which may contain fixed length and variable length fields.

The description of the various parts is contained in the following sections. SCCP Management messages and codes are provided in § 5 of this Recommendation.

#### 1.1 *Routing label*

The standard routing label specified in Recommendation Q.704, § 2.2 is used. The rules for the generation of the signalling link selection (SLS) code are described in Recommendation Q.711, § 2.2.1.

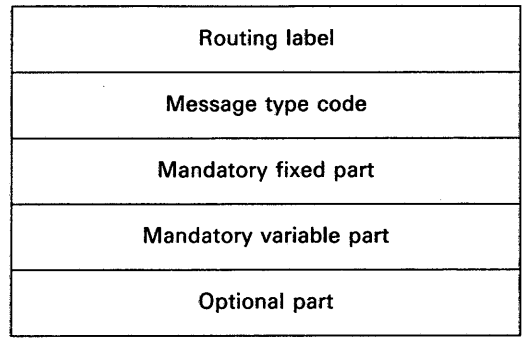



FIGURE 1/Q.713

**General layout**

1.2 *Message type code*

The message type code consists of a one octet field, and is mandatory for all messages. The message type code uniquely defines the function and format of each SCCP message. The allocation of message type codes, with reference to the appropriate descriptive section of this Recommendation is summarized in Table 1/Q.713. Table 1/Q.713 also contains an indication of the applicability of the various message types to the relevant classes of protocol.

1.3 *Formatting principles*

Each message consists of a number of parameters listed and described in § 3. Each parameter has a "name" which is coded as a single octet (see § 3). The length of a parameter may be fixed or variable, and a "length indicator" of one octet for each parameter may be included as described below.

The detailed format is uniquely defined for each message type as described in § 4.

A general SCCP message format is shown in Figure 2/Q.713.

1.4 *Mandatory fixed part*

Those parameters that are mandatory and of fixed length for a particular message type will be contained in the "mandatory fixed part". The position, length and order of the parameters is uniquely defined by the message type. Thus the names of the parameters and the length indicators are not included in the message.

1.5 *Mandatory variable part*

Mandatory parameters of variable length will be included in the mandatory variable part. The name of each parameter and the order in which the pointers are sent is implicit in the message type. Parameter names are, therefore, not included in the message. A pointer is used to indicate the beginning of each parameter. Because of this, parameters may be sent in an order different from that of the pointers. Each pointer is encoded as a single octet. The details of how pointers are encoded is found in § 2.3. The number of parameters, and thus the number of pointers is uniquely defined by the message type.

A pointer is also included to indicate the beginning of the optional part. If the message type indicates that no optional part is allowed, then this pointer will not be present. If the message type indicates that an optional part is possible, but there is no optional part included in this particular message, then a pointer field containing all zeros will be used.

All the pointers are sent consecutively at the beginning of the mandatory variable part. Each parameter contains the parameter length indicator followed by the contents of the parameter.

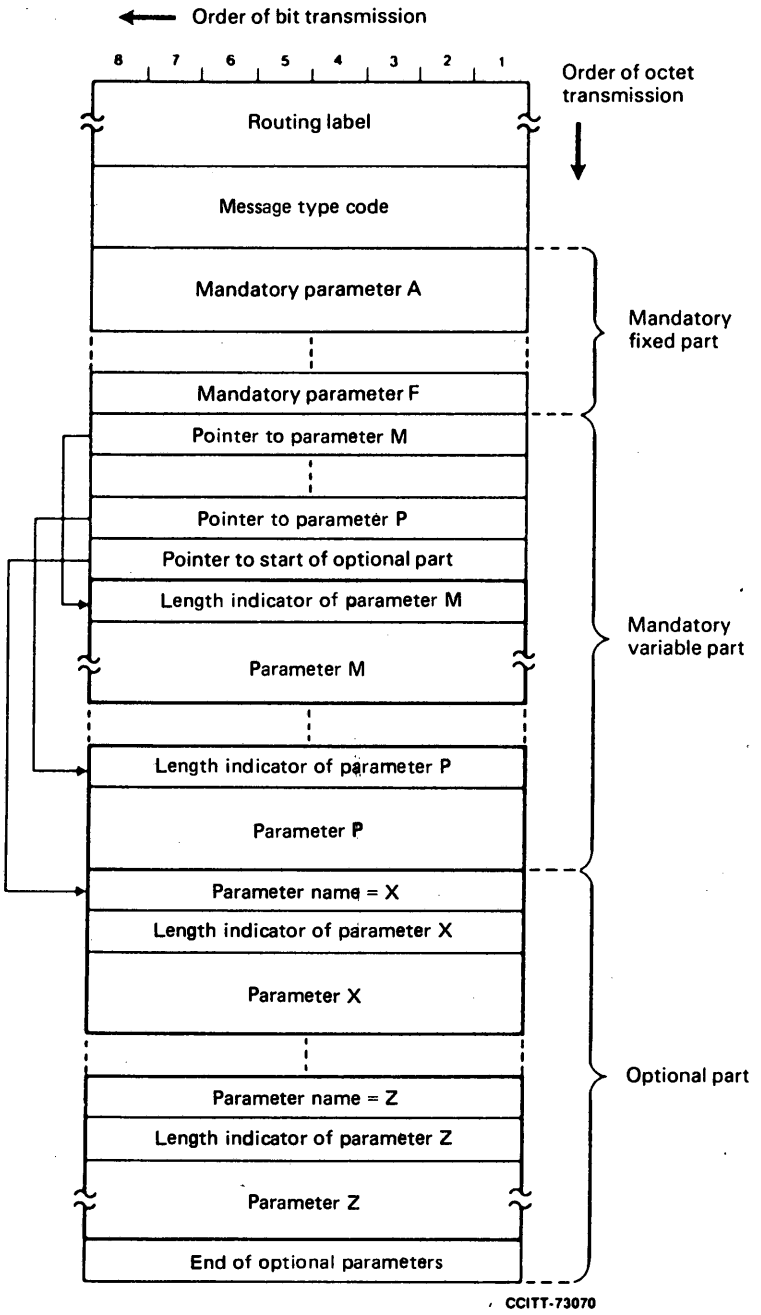



FIGURE 2/Q.713

**General SCCP message format**

## 1.6 *Optional part*

The optional part consists of parameters that may or may not occur in any particular message type. Both fixed length and variable length parameters may be included. Optional parameters may be transmitted in any order[1]. Each optional parameter will include the parameter name (one octet) and the length indicator (one octet) followed by the parameter contents.

[1] It is for further study if any constraint in the order of transmission will be introduced.

1.7 *End of optional parameters octet*

After all optional parameters have been sent, an end of optional parameters octet containing all zeroes will be transmitted. This octet is only included if optional parameters are present in the message.

1.8 *Order of transmission*

Since all the parameters consist of an integral number of octets, the formats are presented as a stack of octets. The first octet transmitted is the one shown at the top of the stack and the last is the one at the bottom (see Figure 2/Q.713).

Within each octet, the bits are transmitted with the least significant bit first.

1.9 *Coding of spare bits*

According to the general rules defined in Rec. Q.700, spare bits are coded 0 unless indicated otherwise at the originating nodes. At intermediate nodes, they are passed transparently. At destination nodes, they need not be examined.

1.10 *National message types and parameters*

If message type codes and parameter codes are required for national uses, it is suggested that the codes be selected from the highest code downwards, that is starting at code 11111110. Code 11111111 is reserved for future use.

## 2 Coding of the general parts

2.1 *Coding of the message type*

The coding of the message is shown in Table 1/Q.713.

2.2 *Coding of the length indicator*

The length indicator field is binary coded to indicate the number of octets in the parameter content field. The length indicator does not include the parameter name octet or the length indicator octet.

2.3 *Coding of the pointers*

The pointer value (in binary) gives the number of octets between the pointer itself (included) and the first octet (not included) of the parameter associated with that pointer[2)].

The pointer value all zeros is used to indicate that, in the case of optional parameters, no optional parameter is present.

## 3 SCCP parameters

The parameter name codes are given in Table 2/Q.713 with reference to the subsections in which they are described.

3.1 *End of optional parameters*

The "end of optional parameters" parameter field consists of a single octet containing all zeros.

3.2 *Destination local reference*

The "destination local reference" parameter field is a three-octet field containing a reference number which, in outgoing messages, has been allocated to the connection section by the remote node.

The coding "all ones" is reserved, its use is for further study.

---

[2)] For example, a pointer value of "00000001" indicates that the associated parameter begins in the octet immediately following the pointer. A pointer value of "00001010" indicates that nine octets of information exist between the pointer octet and the first octet of the parameter associated with that pointer.

TABLE 1/Q.713

**SCCP message types**

| Message type | Classes | | | | § | Code |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | | |
| CR Connection Request | | | X | X | 4.2 | 0000 0001 |
| CC Connection Confirm | | | X | X | 4.3 | 0000 0010 |
| CREF Connection Refused | | | X | X | 4.4 | 0000 0011 |
| RLSD Released | | | X | X | 4.5 | 0000 0100 |
| RLC Release Complete | | | X | X | 4.6 | 0000 0101 |
| DT1 Data Form 1 | | | X | | 4.7 | 0000 0110 |
| DT2 Data Form 2 | | | | X | 4.8 | 0000 0111 |
| AK Data Acknowledgement | | | | X | 4.9 | 0000 1000 |
| UDT Unitdata | X | X | | | 4.10 | 0000 1001 |
| UDTS Unitdata Service | X | X | | | 4.11 | 0000 1010 |
| ED Expedited Data | | | | X | 4.12 | 0000 1011 |
| EA Expedited Data Acknowledgement | | | | X | 4.13 | 0000 1100 |
| RSR Reset Request | | | | X | 4.14 | 0000 1101 |
| RSC Reset Confirm | | | | X | 4.15 | 0000 1110 |
| ERR Protocol Data Unit Error | | | X | X | 4.16 | 0000 1111 |
| IT Inactivity Test | | | X | X | 4.17 | 0001 0000 |

X Type of message in this protocol class.

TABLE 2/Q.713

**SCCP parameter name codes**

| Parameter name | § | Parameter name code 8765 4321 |
|---|---|---|
| End of optional parameters | 3.1 | 0000 0000 |
| Destination local reference | 3.2 | 0000 0001 |
| Source local reference | 3.3 | 0000 0010 |
| Called party address | 3.4 | 0000 0011 |
| Calling party address | 3.5 | 0000 0100 |
| Protocol class | 3.6 | 0000 0101 |
| Segmenting/reassembling | 3.7 | 0000 0110 |
| Receive sequence number | 3.8 | 0000 0111 |
| Sequencing/segmenting | 3.9 | 0000 1000 |
| Credit | 3.10 | 0000 1001 |
| Release cause | 3.11 | 0000 1010 |
| Return cause | 3.12 | 0000 1011 |
| Reset cause | 3.13 | 0000 1100 |
| Error cause | 3.14 | 0000 1101 |
| Refusal cause | 3.15 | 0000 1110 |
| Data | 3.16 | 0000 1111 |

3.3 *Source local reference*

The "source local reference" parameter field is a three-octet field containing a reference number which is generated and used by the local node to identify the connection section.

The coding "all ones" is reserved, its use is for further study.

3.4 *Called party address*

The "called party address" is a variable length parameter. Its structure is shown in Figure 3/Q.713.

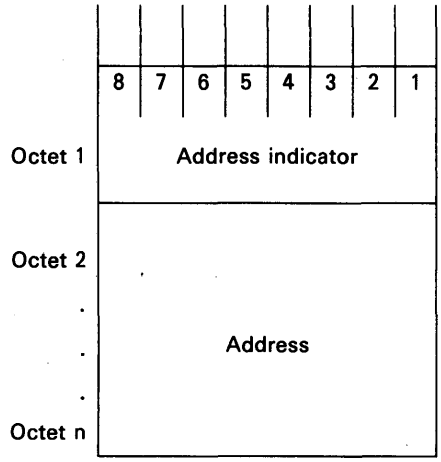



FIGURE 3/Q.713

**Called/Calling party address**

3.4.1 *Address indicator*

The "address indicator" indicates the type of address information contained in the address field (see Figure 4/Q.713). The address consists of one or any combination of the following elements:

- signalling point code;
- global title (for instance, dialled digits);
- subsystem number.

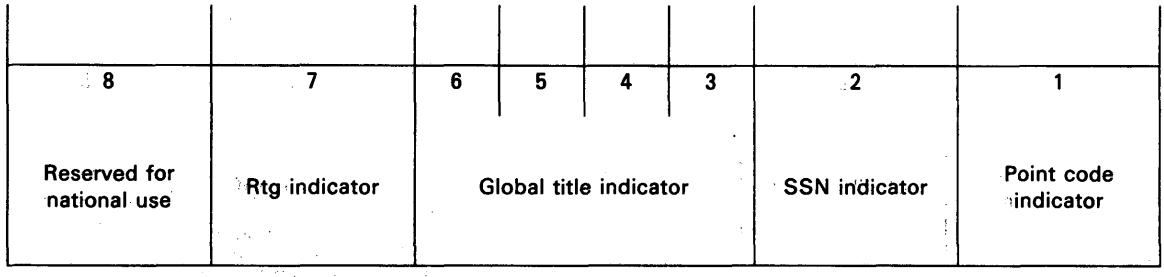



FIGURE 4/Q.713

**Address indicator encoding**

A "1" in bit 1 indicates that the address contains a signalling point code.

A "1" in bit 2 indicates that the address contains a subsystem number.

Bits 3-6 of the address indicator octet contain the global title indicator, which is encoded as follows:

| Bits 6 5 4 3 | |
|---|---|
| 0 0 0 0 | No global title included |
| 0 0 0 1 | Global title includes nature of address indicator only |
| 0 0 1 0 | Global title includes translation type only[3] |
| 0 0 1 1 | Global title includes translation type, numbering plan and encoding scheme[3] |
| 0 1 0 0 | Global title includes translation type, numbering plan, encoding scheme and nature of address indicator |
| 0 1 0 1 to 0 1 1 1 | spare international |
| 1 0 0 0 to 1 1 1 0 | spare national |
| 1 1 1 1 | reserved for extension. |

When a global title is used in the called party address, it is suggested that the called party address contain a subsystem number. This serves to simplify message reformatting following global title translation. The subsystem number should be encoded "00000000" when the subsystem number is not known, e.g., before translation.

Bit 7 of the address indicator octet contains routing information identifying which address element should be used for routing.

A "0" in bit 7 indicates that routing should be based on the global title in the address.

A "1" in bit 7 indicates that routing should be based on the destination point code in the MTP routing label and the subsystem number information in the called party address.

Bit 8 of the address indicator octet is designated for national use.

### 3.4.2 *Address*

The various elements, when provided, occur in the order: point code, subsystem number, global title, as shown in Figure 5/Q.713.

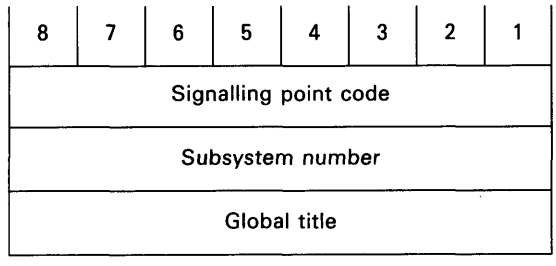



FIGURE 5/Q.713

**Ordering of address elements**

[3] Full E.164 numbering plan address is used in these two cases for Recommendation E.164 based global titles.

3.4.2.1 *Signalling point code*

The signalling point code, when provided, is represented by two octets. Bits 7 and 8 in the second octet are set to zero (see Figure 6/Q.713).

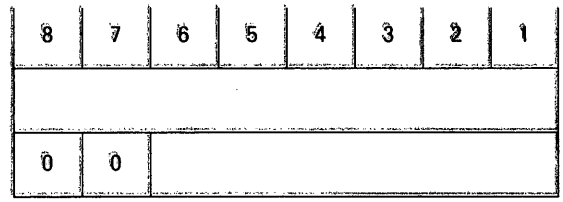



FIGURE 6/Q.713

**Signalling point code encoding**

3.4.2.2 *Subsystem number*

The subsystem number (SSN) identifies an SCCP user function and, when provided, consists of one octet coded as follows:

| Bits 8 7 6 5 4 3 2 1 | |
|---|---|
| 0 0 0 0 0 0 0 0 | SSN not known/not used |
| 0 0 0 0 0 0 0 1 | SCCP management |
| 0 0 0 0 0 0 1 0 | reserved for CCITT allocation |
| 0 0 0 0 0 0 1 1 | ISDN user part |
| 0 0 0 0 0 1 0 0 | OMAP |
| 0 0 0 0 0 1 0 1 | MAP (Mobile Application Part) |
| 0 0 0 0 0 1 1 0 to 1 1 1 1 1 1 1 0 | spare |
| 1 1 1 1 1 1 1 1 | reserved for expansion. |

Network specific subsystem numbers should be assigned in descending order starting with "11111110".

3.4.2.3 *Global title* [4]

The format of the global title is of variable length. Figure 7/Q.913, Figure 9/Q.713, Figure 10/Q.713 and Figure 11/Q.713 show four possible formats for global title.

[4] Incorporation of NSAP address in the SCCP global title is for further study.

3.4.2.3.1 *Global title indicator = 0001*

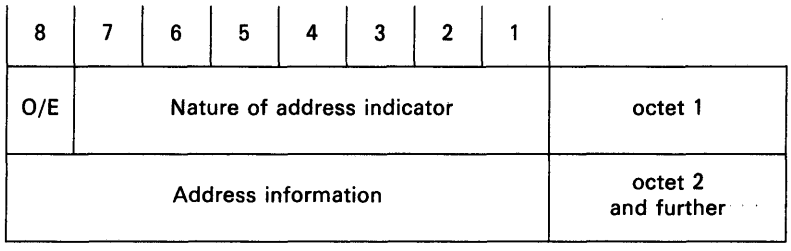



FIGURE 7/Q.713

**Global title format for indicator 0001**

Bits 1 to 7 of octet 1 contain the nature of address indicator and are coded as follows:

Bits 7 6 5 4 3 2 1

| | |
|---|---|
| 0 0 0 0 0 0 0 | spare |
| 0 0 0 0 0 0 1 | subscriber number |
| 0 0 0 0 0 1 0 | reserved for national use |
| 0 0 0 0 0 1 1 | national significant number |
| 0 0 0 0 1 0 0 | international number |
| 0 0 0 0 1 0 1 to 1 1 1 1 1 1 1 | spare |

Bit 8 of octet 1 contains the odd/even indicator and is coded as follows:

Bit 8

0 even number of address signals
1 odd number of address signals

The octets 2 and further contain a number of address signals and possibly a filler as shown in Figure 8/Q.713.

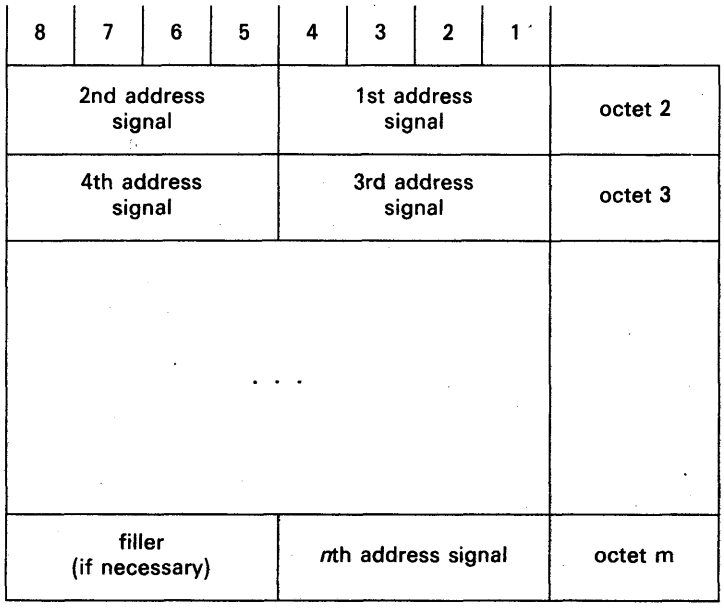



FIGURE 8/Q.713

**Address information**

Each address signal is coded as follows:

0000 digit 0
0001 digit 1
0010 digit 2
0011 digit 3
0100 digit 4
0101 digit 5
0110 digit 6
0111 digit 7
1000 digit 8
1001 digit 9
1010 spare
1011 code 11[5)]
1100 code 12[5)]
1101 spare
1110 spare
1111 ST[5)]

In case of an odd number of address signals, a filler code 0000 is inserted after the last address signal.

3.4.2.3.2 *Global title indicator = 0010*

Figure 9/Q.713 shows the format of the global title, if the global title indicator equals "0010".

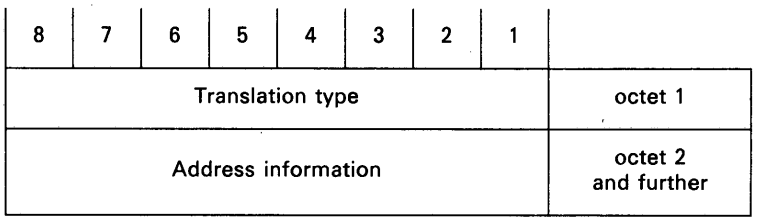



FIGURE 9/Q.713

**Global title format for indicator 0010**

The translation type is a one-octet field that is used to direct the message to the appropriate global title translation function.[6)] Thus, it may be possible for the address information to be translated into different values for and different combinations of DPCs, SSNs and GTs.

This octet will be coded "00000000" when not used. Translation types for internetwork services will be assigned in ascending order starting with 00000001". Translation types for network specific services will be assigned in descending order starting with "11111110". The code "11111111" is reserved for expansion. However, the exact coding of translation types in the international network is for further study. Additional requirements may be placed on this field as a result of further work on Transaction Capabilities and the ISDN User Part.

In the case of this global title format (0010), the translation type may also imply the encoding scheme, used to encode the address information, and the numbering plan.

---

5) The application of these codes in actual networks is for further study.

6) A translation type may for instance imply a specific service to be provided by the SCCP user, such as free phone number translation, or identify the category of service to be provided, for example, dialed number screening, password validation or transmission of digits to telephone network address.

3.4.2.3.3 *Global title indicator = 0011*

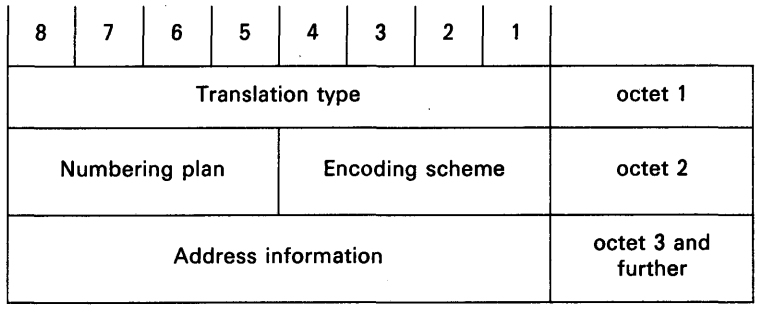



FIGURE 10/Q.713

**Global title format for indicator 0011**

The translation type is as described in § 3.4.2.3.2.

The numbering plan is encoded as follows[7]:

| Bits 8 7 6 5 | |
|---|---|
| 0 0 0 0 | unknown |
| 0 0 0 1 | ISDN/Telephony Numbering Plan (Recommendations E.163 and E.164) |
| 0 0 1 0 | spare |
| 0 0 1 1 | Data Numbering Plan (Recommendation X.121) |
| 0 1 0 0 | Telex Numbering Plan (Recommendation F.69) |
| 0 1 0 1 | Maritime Mobile Numbering Plan (Recommendations E.210, 211) |
| 0 1 1 0 | Land Mobile Numbering Plan (Recommendation E.212) |
| 0 1 1 1 | ISDN/Mobile numbering plan (Recommendation E.214) |
| 1 0 0 0 to 1 1 1 0 | spare |
| 1 1 1 1 | reserved |

The encoding scheme is encoded as follows:

| Bits 4 3 2 1 | |
|---|---|
| 0 0 0 0 | unknown |
| 0 0 0 1 | BCD, odd number of digits |
| 0 0 1 0 | BCD, even number of digits |
| 0 0 1 1 to 1 1 1 0 | spare |
| 1 1 1 1 | reserved. |

If the encoding scheme is binary coded decimal, the global title value, starting from octet 3, is encoded as shown in Figure 8/Q.713.

[7] The support of all numbering plans is not mandatory.

3.4.2.3.4 *Global title indicator = 0100*

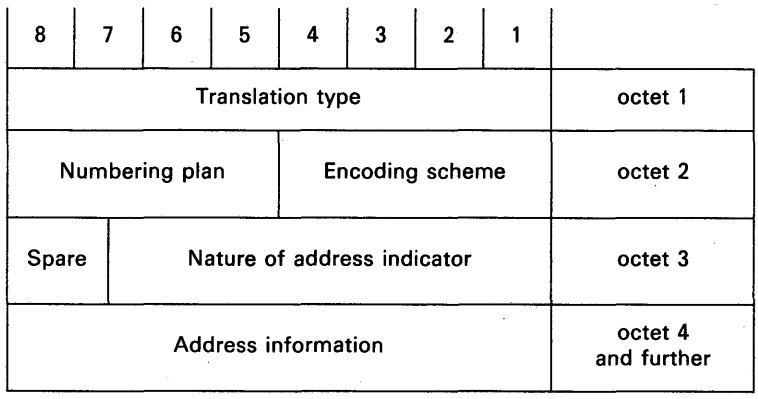



FIGURE 11/Q.713

**Global title format for indicator 0100**

The field "translation type" is as described in § 3.4.2.3.2. The fields "numbering plan" and "encoding scheme" are as described in § 3.4.2.3.3. The field "nature of address indicator" is as described in § 3.4.2.3.1.

If the encoding scheme is binary coded decimal, the global title value, starting from octet 4, is encoded as shown in Figure 8/Q.713.

## 3.5 *Calling party address*

The "calling party address" is a variable length parameter. Its structure is the same as the "called party address".

When the calling party address is a mandatory parameter but is not available or must not be sent, the calling party address parameter only consists of the address indicator octet, where bits 1 to 7 are coded all zeros.

## 3.6 *Protocol class*

The "protocol class" parameter field is a four bit field containing the protocol class.

Bits 1-4 are coded as follows:

4321
0000 class 0
0001 class 1
0010 class 2
0011 class 3

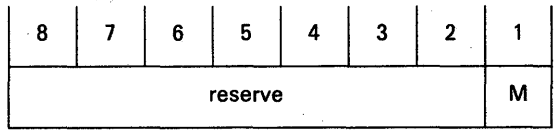
When bits 1-4 are coded to indicate a connection-oriented-protocol class (class 2, class 3), bits 5-8 are spare.

When bits 1-4 are coded to indicate a connectionless protocol class (class 0, class 1), bits 5-8 are used to specify message handling as follows:

| Bits 8 7 6 5 | |
|---|---|
| 0 0 0 0 | no special options |
| 0 0 0 1 to 0 1 1 1 | spare |
| 1 0 0 0 | return message on error |
| 1 0 0 1 to 1 1 1 1 | spare |

3.7 *Segmenting/reassembling*

The "segmenting/reassembling" parameter field is a one octet field and is structured as follows:




Bits 8-2 are spare.

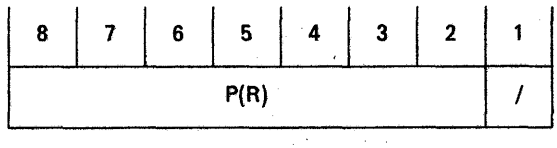
Bit 1 is used for the More Data indication and is coded as follows:

0 = no more data

1 = more data

3.8 *Receive sequence number*

The "receive sequence number" parameter field is a one octet field and is structured as follows:

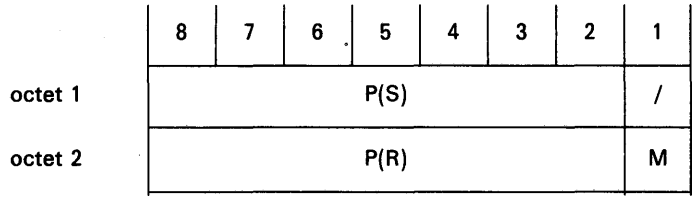



Bits 8-2 contain the receive sequence number P(R) used to indicate the sequence number of the next expected message. P(R) is binary coded and bit 2 is the LSB.

Bit 1 is spare.

3.9 *Sequencing/segmenting*

The sequencing/segmenting parameter field consists of two octets and is structured as follows:




Bits 8-2 of octet 1 are used for indicating the send sequence number P(S). P(S) is binary coded and bit 2 is the LSB.

Bit 1 of octet 1 is spare.

Bits 8-2 of octet 2 are used for indicating the receive sequence number P(R). P(R) is binary coded and bit 2 is the LSB.

Bit 1 of octet 2 is used for the More Data indication and is coded as follows:

0 = no more data

1 = more data

The sequencing/segmenting parameter field is used exclusively in protocol class 3.

3.10 *Credit*

The "credit" parameter field is a one-octet field used in the protocol classes which include flow control functions. It contains the window size value coded in pure binary.

3.11 *Release cause*

The release cause parameter field is a one-octet field containing the reason for the release of the connection.

The coding of the release cause field is as follows:

| Bits 8 7 6 5 4 3 2 1 | |
|---|---|
| 0 0 0 0 0 0 0 0 | end user originated |
| 0 0 0 0 0 0 0 1 | end user congestion |
| 0 0 0 0 0 0 1 0 | end user failure |
| 0 0 0 0 0 0 1 1 | SCCP user originated |
| 0 0 0 0 0 1 0 0 | remote procedure error |
| 0 0 0 0 0 1 0 1 | inconsistent connection data |
| 0 0 0 0 0 1 1 0 | access failure |
| 0 0 0 0 0 1 1 1 | access congestion |
| 0 0 0 0 1 0 0 0 | subsystem failure |
| 0 0 0 0 1 0 0 1 | subsystem congestion [8] |
| 0 0 0 0 1 0 1 0 | network failure |
| 0 0 0 0 1 0 1 1 | network congestion |
| 0 0 0 0 1 1 0 0 | expiration of reset timer |
| 0 0 0 0 1 1 0 1 | expiration of receive inactivity timer |
| 0 0 0 0 1 1 1 0 | not obtainable |
| 0 0 0 0 1 1 1 1 | unqualified |
| 0 0 0 1 0 0 0 0 to 1 1 1 1 1 1 1 1 | spare |

*Note* – A more comprehensive list of causes covering X.96 call progress information is for further study.

[8] Subsystem congestion control procedure is for further study.

3.12 *Return cause*

In the *Unitdata Service* message, the «return cause» parameter field is a one octet field containing the reason for message return. Bits 1-8 are coded as follows:

| Bits 8 7 6 5 4 3 2 1 | |
|---|---|
| 0 0 0 0 0 0 0 0 | no translation for an address of such nature |
| 0 0 0 0 0 0 0 1 | no translation for this specific address |
| 0 0 0 0 0 0 1 0 | subsystem congestion [9] |
| 0 0 0 0 0 0 1 1 | subsystem failure |
| 0 0 0 0 0 1 0 0 | unequipped user |
| 0 0 0 0 0 1 0 1 | network failure |
| 0 0 0 0 0 1 1 0 | network congestion |
| 0 0 0 0 0 1 1 1 | unqualified |
| 0 0 0 0 1 0 0 0 to 1 1 1 1 1 1 1 1 | spare |

3.13 . *Reset cause*

The "reset cause" parameter field is a one octet field containing the reason for the resetting of the connection.

The coding of the reset cause field is as follows:

| Bits 8 7 6 5 4 3 2 1 | |
|---|---|
| 0 0 0 0 0 0 0 0 | end user originated |
| 0 0 0 0 0 0 0 1 | SCCP user originated |
| 0 0 0 0 0 0 1 0 | message out of order – incorrect P(S) |
| 0 0 0 0 0 0 1 1 | message out of order – incorrect P(R) |
| 0 0 0 0 0 1 0 0 | remote procedure error – message out of window |
| 0 0 0 0 0 1 0 1 | remote procedure error – incorrect P(S) after (re)initialization |
| 0 0 0 0 0 1 1 0 | remote procedure error – general |
| 0 0 0 0 0 1 1 1 | remote end user operational |
| 0 0 0 0 1 0 0 0 | network operational |
| 0 0 0 0 1 0 0 1 | access operational |
| 0 0 0 0 1 0 1 0 | network congestion |
| 0 0 0 0 1 0 1 1 | not obtainable |
| 0 0 0 0 1 1 0 0 | unqualified |
| 0 0 0 0 1 1 0 1 to 1 1 1 1 1 1 1 1 | spare |

3.14 *Error cause*

The "error cause" parameter field is a one octet field containing the indication of the exact protocol error.

The coding of the error cause field is as follows:

| Bits 8 7 6 5 4 3 2 1 | |
|---|---|
| 0 0 0 0 0 0 0 0 | local reference number (LRN) mismatch – unassigned destination LRN |
| 0 0 0 0 0 0 0 1 | local reference number (LRN) mismatch – inconsistent source LRN |
| 0 0 0 0 0 0 1 0 | point code mismatch [10] |
| 0 0 0 0 0 0 1 1 | service class mismatch |
| 0 0 0 0 0 1 0 0 | unqualified |
| 0 0 0 0 0 1 0 1 to 1 1 1 1 1 1 1 1 | spare |

[9] Subsystem congestion control procedure is for further study.

[10] National option.

3.15 *Refusal cause*

The refusal cause parameter field is a one octet field containing the reason for the refusal of the connection.

The coding of the refusal cause field is as follows:

| Bits 8 7 6 5 4 3 2 1 | |
|---|---|
| 0 0 0 0 0 0 0 0 | end user originated |
| 0 0 0 0 0 0 0 1 | end user congestion |
| 0 0 0 0 0 0 1 0 | end user failure |
| 0 0 0 0 0 0 1 1 | SCCP user originated |
| 0 0 0 0 0 1 0 0 | destination address unknown |
| 0 0 0 0 0 1 0 1 | destination inaccessible |
| 0 0 0 0 0 1 1 0 | network resource – QOS not available/non-transient |
| 0 0 0 0 0 1 1 1 | network resource – QOS not available/transient |
| 0 0 0 0 1 0 0 0 | access failure |
| 0 0 0 0 1 0 0 1 | access congestion |
| 0 0 0 0 1 0 1 0 | subsystem failure |
| 0 0 0 0 1 0 1 1 | subsystem congestion [11] |
| 0 0 0 0 1 1 0 0 | expiration of the connection establishment timer |
| 0 0 0 0 1 1 0 1 | incompatible user data |
| 0 0 0 0 1 1 1 0 | not obtainable |
| 0 0 0 0 1 1 1 1 | unqualified |
| 0 0 0 1 0 0 0 0 to 1 1 1 1 1 1 1 1 | spare |

*Note 1* – The inclusion of the routing failure causes as specified for the "return cause" parameter in Recommendation Q.713, § 3.12, is for further study.

*Note 2* – A more comprehensive list of causes covering CCITT Recommendation X.96 call progress information is for further study.

3.16 *Data*

The "data" parameter field is a variable length field containing SCCP-user data to be transferred transparently between the SCCP user functions.

## 4 SCCP messages and codes

### 4.1 *General*

4.1.1 In the following sections, the format and coding of the SCCP messages is specified.

For each message a list of the relevant parameters is given in a tabular form.

4.1.2 For each parameter the table also includes:

- *a reference* to the section where the formatting and coding of the parameter content is specified;
- *the type* of the parameter. The following types are used in the tables:
  - F = mandatory fixed length parameter;
  - V = mandatory variable length parameter;
  - O = optional parameter of fixed or variable length;
- *the length* of the parameter. The value in the table includes:
  - *for type F parameters* the length, in octets, of the parameter content;
  - *for type V parameters* the length, in octets, of the length indicator and of the parameter content; (The minimum and the maximum length are indicated.)
  - *for type O parameters* the length, in octets, of the parameter name, length indicator and parameter content. (For variable length parameters the minimum and maximum length is indicated.)

[11] Subsystem congestion control procedure is for further study.

4.1.3 For each message the number of pointers included is also specified.

4.1.4 For each message type, type F parameters and the pointers for the type V parameters must be sent in the order specified in the following tables.

### 4.2 *Connection request (CR)*

The CR message contains:
- the routing label,
- 2 pointers,
- the parameters indicated in Table 3/Q.713.

### 4.3 *Connection confirm (CC)*

The CC message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 4/Q.713.

### 4.4 *Connection refused (CREF)*

The message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 5/Q.713.

### 4.5 *Released (RLSD)*

The RLSD message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 6/Q.713.

### 4.6 *Release complete (RLC)*

The RLC message contains:
- the routing label,
- no pointers,
- the parameters indicated in Table 7/Q.713.

### 4.7 *Data form 1 (DT1)*

The DT1 message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 8/Q.713.

### 4.8 *Data form 2 (DT2)*

The DT2 message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 9/Q.713.

TABLE 3/Q.713

**Message type: Connection request**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type code | 2.1 | F | 1 |
| Source local reference | 3.3 | F | 3 |
| Protocol class | 3.6 | F | 1 |
| Called party address | 3.4 | V | 3 minimum |
| Credit | 3.10 | O | 3 |
| Calling party address | 3.5 | O | 4 minimum |
| Data | 3.16 | O | 3 - 130 |
| End of optional parameters | 3.1 | O | 1 |

TABLE 4/Q.713

**Message type: Connection confirm**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Source local reference | 3.3 | F | 3 |
| Protocol class | 3.6 | F | 1 |
| Credit | 3.10 | O | 3 |
| Called party address | 3.4 | O | 4 minimum |
| Data | 3.16 | O | 3 - 130 |
| End of optional parameter | 3.1 | O | 1 |

TABLE 5/Q.713

**Message type: Connection refused**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Refusal cause | 3.15 | F | 1 |
| Called party address | 3.4 | O | 4 minimum |
| Data | 3.16 | O | 3 - 130 |
| End of optional parameter | 3.1 | O | 1 |

TABLE 6/Q.713

**Message type: Released**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Source local reference | 3.3 | F | 3 |
| Release cause | 3.11 | F | 1 |
| Data | 3.16 | O | 3 - 130 |
| End of optional parameter | 3.1 | O | 1 |

TABLE 7/Q.713

**Message type: Release complete**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Source local reference | 3.3 | F | 3 |

TABLE 8/Q.713

**Message type: Data form 1**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Segmenting/reassembling | 3.7 | F | 1 |
| Data | 3.16 | V | 2 - 256 |

TABLE 9/Q.713

**Message type: Data form 2**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Sequencing/Segmenting | 3.9 | F | 2 |
| Data | 3.16 | V | 2 - 256 |

4.9 *Data acknowledgement (AK)*

The AK message contains:
- the routing label,
- no pointers,
- the parameters indicated in Table 10/Q.713.

TABLE 10/Q.713

**Message type: Data acknowledgement**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Receive sequence number | 3.8 | F | 1 |
| Credit | 3.10 | F | 1 |

4.10 *Unitdata (UDT)*

The UDT message contains:
- the routing label,
- 3 pointers,
- the parameters indicated in Table 11/Q.713.

TABLE 11/Q.713

**Message type: Unitdata**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Protocol class | 3.6 | F | 1 |
| Called party address | 3.4 | V | 3 minimum |
| Calling party address | 3.5 | V | 2 minimum |
| Data | 3.16 | V | 2 - X [a] |

[a] Due to the ongoing studies on the SCCP called and calling party address, the maximum length of this parameter needs further study. It is also noted that the transfer of up to 255 octets of user data is allowed when the SCCP called and calling party address do not include global title.

4.11 *Unitdata service (UDTS)*

The UDTS message contains:
- the routing label,
- 3 pointers,
- the parameters indicated in Table 12/Q.713.

TABLE 12/Q.713

**Message type: Unitdata service**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Return cause | 3.12 | F | 1 |
| Called party address | 3.4 | V | 3 minimum |
| Calling party address | 3.5 | V | 2 minimum |
| Data | 3.16 | V | 2 - X [a] |

[a] See [a] Table 11/Q.713.

4.12 *Expedited data (ED)*

The ED message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 13/Q.713.

TABLE 13/Q.713

**Message type: Expedited data**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Data | 3.16 | V | 2 - 33 |

4.13 *Expedited data acknowledgement (EA)*

The EA message contains:
- the routing label,
- no pointers,
- the parameters indicated in Table 14/Q.713.

TABLE 14/Q.713

**Message type: Expedited data acknowledgement**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |

4.14 *Reset request (RSR)*

The RSR message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 15/Q.713.

TABLE 15/Q.713

**Message type: Reset request**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Source local reference | 3.3 | F | 3 |
| Reset cause | 3.13 | F | 1 |

4.15 *Reset confirm (RSC)*

The RSC message contains:
- the routing label,
- no pointers,
- the parameters indicated in Table 16/Q.713.

TABLE 16/Q.713

**Message type: Reset confirmation**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Source local reference | 3.3 | F | 3 |

4.16 *Protocol data unit error (ERR)*

The ERR message contains:
- the routing label,
- 1 pointer,
- the parameters indicated in Table 17/Q.713.

TABLE 17/Q.713

**Message type: Protocol data unit error**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Error cause | 3.14 | F | 1 |

4.17 *Inactivity test (IT)*

The IT message contains:

- the routing label,
- no pointers,
- the parameters indicated in Table 18/Q.713.

TABLE 18/Q.713

**Message type: Inactivity test**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type | 2.1 | F | 1 |
| Destination local reference | 3.2 | F | 3 |
| Source local reference | 3.3 | F | 3 |
| Protocol class | 3.6 | F | 1 |
| Sequencing/segmenting [a)] | 3.9 | F | 2 |
| Credit [a)] | 3.10 | F | 1 |

[a)] Information in these parameter fields reflect those values sent in the last data Form 2 or Data acknowledgement message. They are ignored if the protocol class parameter indicates class 2.

## 5 SCCP Management messages and codes

### 5.1 *General*

SCCP Management (SCMG) messages are carried using the connectionless service of the SCCP. When transferring SCMG messages, class 0 is requested with the "discard message on error" option. SCCP management message parts are provided in the "data" parameter of the *Unitdata message.*

The *Unitdata* message contains:

- the routing label,
- 3 pointers,
- the parameters indicated in Table 19/Q.713.

Descriptions of the various parts are contained in the following sections.

TABLE 19/Q.713

**SCCP management message format**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| Message type<br>(= Unitdata) | 2.1 | F | 1 |
| Protocol class<br>(= Class 0, no return) | 3.6 | F | 1 |
| Called party address<br>(SSN = SCCP management) | 3.4 | V | 3 minimum |
| Calling party address<br>(SSN = SCCP management) | 3.5 | V | 3 minimum [a] |
| Data<br>(Data consists of an SCMG message with form as in Table 22/Q.713) | 3.16 | V | 6 |

[a] SSN is always present.

5.1.1 *SCMG format identifier*

The SCMG format identifier consists of a one-octet field, which is mandatory for all SCMG messages. The SCMG format identifier uniquely defines the function and format of each SCMG message. The allocation of SCMG format identifiers is shown in Table 20/Q.713.

TABLE 20/Q.713

**SCMG format identifiers**

| Message | Code<br>87654321 |
|---|---|
| SSA Subsystem-Allowed | 00000001 |
| SSP Subsystem-Prohibited | 00000010 |
| SST Subsystem-Status-Test | 00000011 |
| SOR Subsystem-Out-of-Service-Request | 00000100 |
| SOG Subsystem-Out-of-Service-Grant | 00000101 |

### 5.1.2 *Formatting principles*

The formatting principles used for SCCP messages, as described in §§ 1.3, 1.4, 1.5, 1.6, 2.2 and 2.3 apply to SCMG messages.

## 5.2 *SCMG message parameters*

SCMG parameter name codes are given in Table 21/Q.713 with reference to the subsections in which they are described. Presently, these parameter name codes are not used since all SCMG messages contain mandatory fixed parameters only.

TABLE 21/Q.713

**SCMG parameter name codes**

| Parameter name | § | Parameter name code 87654321 |
|---|---|---|
| End of optional parameters | 5.2.1 | 00000000 |
| Affected SSN | 5.2.2 | 00000001 |
| Affected PC | 5.2.3 | 00000010 |
| Subsystem multiplicity indicator | 5.2.4 | 00000011 |

### 5.2.1 *End of optional parameters*

The "end of optional parameters" parameter field consists of a single octet containing all zeros.

### 5.2.2 *Affected SSN*

The "affected subsystem number (SSN)" parameter field consists of one octet coded as directed for the called party address field, § 3.4.2.1.

### 5.2.3 *Affected PC*

The "affected signalling point code (PC)" parameter field is represented by two octets which are coded as directed for the called party address field, § 3.4.2.2.

### 5.2.4 *Subsystem multiplicity indicator*

The "subsystem multiplicity indicator" parameter field consists of one octet coded as shown in Figure 12/Q.713.

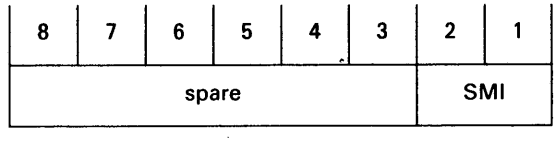



FIGURE 12/Q.713

**Subsystem multiplicity indicator format**

The coding of the SMI field is as follows:

Bits 21

| | |
|---|---|
| 00 | affected subsystem multiplicity unknown |
| 01 | affected subsystem is solitary |
| 10 | affected subsystem is duplicated |
| 11 | spare |

Bits 3-8 are spare.

## 5.3 *SCMG messages*

Presently, all SCMG messages contain mandatory fixed parameters only. Each SCMG message contains:

- 0 pointers
- the parameters indicated in Table 22/Q.713.

TABLE 22/Q.713

**SCMG Message**

| Parameter | § | Type (F V O) | Length (octets) |
|---|---|---|---|
| SCMG format identifier (Message type code) | 5.1.1 | F | 1 |
| Affected SSN | 5.2.2 | F | 1 |
| Affected PC | 5.2.3 | F | 2 |
| Subsystem multiplicity indicator | 5.2.4 | F | 1 |

# ANNEX A

(to Recommendation Q.713)

## Mapping for cause parameter values

## A.1 *Introduction*

During connection refusal/release/reset, the SCCP and its users could take necessary corrective actions, if any, only upon relevant information available to them. Thus, it would be very helpful if those information could be conveyed correctly.

During connection release, the "release cause" parameter in the *Released* (RLSD) message and the N-DISCONNECT primitive (with parameters "originator" and "reason") are used together to convey those information on the initiator and the cause of the connection release. In addition, the N-DISCONNECT primitive is also used together with the "refusal cause" parameter in the *Connection Refused* (CREF) message to convey those information during connection refusal. During connection reset, the "reset cause" parameter in the *Reset Request* (RSR) message and the N-RESET primitive (with parameters "originator" and "reason") are used together similarly.

In order to convey those information correctly, this Annex provides a guideline for the mapping of values between the cause parameters and the corresponding N-primitive parameters during various scenarios.

## A.2 *Connection refusal*

Table A-1/Q.713 describes the mapping of values between the "refusal cause" parameter (§ 3.15, Rec. Q.713) and the "originator", "reason" parameters in the N-DISCONNECT primitive (§ 2.1.1.2.4, Rec. Q.711).

## A.3 *Connection release*

Table A-2/Q.713 describes the mapping of values between the "release cause" parameter (§ 3.11, Rec. Q.713) and the "originator", "reason" parameters in the N-DISCONNECT primitive (§ 2.1.1.2.4, Rec. Q.711).

## A.4 *Connection reset*

Table A-3/Q.713 describes the mapping of values between the "reset cause" parameter (§ 3.13, Rec. Q.713) and the "originator", "reason" parameters in the N-RESET primitive (§ 2.1.1.2.3, Rec. Q.711).

TABLE A-1/Q.713

**Mapping during connection refusal**

| CREF Message | | N-DISCONNECT primitive | |
|---|---|---|---|
| Code | Refusal cause | Reason | Originator |
| 00000000 | end user originated | connection refusal – end user originated | NSU |
| 00000001 | end user congestion | connection refusal – end user congestion | NSU |
| 00000010 | end user failure | connection refusal – end user failure | NSU |
| 00000011 | SCCP user originated | connection refusal – SCCP user originated | NSU |
| 00000100 | destination address unknown | connection refusal – destination address unknown (non-transient condition) | NSP |
| 00000101 | destination inaccessible | connection refusal – destination inaccessible/transient condition | NSP |
| 00000110 | network resource – QOS unavailable/non-transient | connection refusal – QOS unavailable/non-transient condition | NSP [a] |
| 00000111 | network resource – QOS unavailable/transient | connection refusal – QOS unavailable/transient condition | NSP [a] |
| 00001000 | access failure | connection refusal – access failure | NSU |
| 00001001 | access congestion | connection refusal – access congestion | NSU |
| 00001010 | subsystem failure | connection refusal – destination inaccessible/non-transient condition | NSP |
| 00001011 | subsystem congestion | connection refusal – subsystem congestion | NSU |
| 00001100 | expiration of connection estimated timer | connection refusal – reason unspecified/transient | NSP [a] |
| 00001101 | inconsistent user data | connection refusal – incompatible information in NSDU | NSU |
| 00001110 | not obtainable | connection refusal – reason unspecified/transient | NSP [a] |
| 00001110 | not obtainable | connection refusal – undefined | undefined |
| 00001111 | unqualified | connection refusal – reason unspecified/transient | NSP [a] |
| 00001111 | unqualified | connection refusal – undefined | undefined |

NSU Network Service User

NSP Network Service Provider

[a] Only those cases will be applicable if the SCCP originates the refusal procedure in response to REQUEST interface element.

TABLE A-2/Q.713

**Mapping during connection release**

| RLSD Message | | N-DISCONNECT primitive | |
|---|---|---|---|
| Code | Release cause | Reason | Originator |
| 00000000 | end user originated | disconnection – normal condition | NSU |
| 00000001 | end user congestion | disconnection – end user congestion | NSU |
| 00000010 | end user failure | disconnection – end user failure | NSU |
| 00000011 | SCCP user originated | disconnection – SCCP user originated | NSU |
| 00000100 | remote procedure error | disconnection – abnormal condition of transient nature | NSP |
| 00000101 | inconsistent connection data | disconnection – abnormal condition of transient nature | NSP |
| 00000110 | access failure | disconnection – access failure | NSU |
| 00000111 | access congestion | disconnection – access congestion | NSU |
| 00001000 | subsystem failure | disconnection – abnormal condition of non-transient nature | NSP |
| 00001001 | subsystem congestion | disconnection – subsystem congestion | NSU |
| 00001010 | network failure | disconnection – abnormal condition of non-transient nature | NSP |
| 00001011 | network congestion | disconnection – abnormal condition of transient nature | NSP |
| 00001100 | expiration of reset timer | disconnection – abnormal condition of transient nature | NSP |
| 00001101 | expiration of receive inactivity timer | disconnection – abnormal condition of transient nature | NSP |
| 00001110 | not obtainable [a] | disconnection – undefined | NSP |
| 00001110 | not obtainable [a] | disconnection – undefined | undefined |
| 00001111 | unqualified | disconnection – abnormal condition | NSU |
| 00001111 | unqualified | disconnection – undefined | NSP |
| 00001111 | unqualified | disconnection – undefined | undefined |

NSU Network Service User

NSP Network Service Provider

[a] The need for this value is for further study.

TABLE A-3/Q.713

**Mapping during connection reset**

| RSR Message | | N-RESET primitive | |
|---|---|---|---|
| Code | Reset cause | Reason | Originator |
| 00000000 | end user originated | reset – user synchronization | NSU |
| 00000001 | SCCP user originated | reset – user synchronization | NSU |
| 00000010 | message out of order – incorrect P(S) | reset – unspecified | NSP |
| 00000011 | message out of order – incorrect P(R) | reset – unspecified | NSP |
| 00000100 | remote procedure error – message out of window | reset – unspecified | NSP |
| 00000101 | remote procedure error – incorrect P(S) after initialization | reset – unspecified | NSP |
| 00000110 | remote procedure error – general | reset – unspecified | NSP |
| 00000111 | remote end user operational | reset – user synchronization | NSU |
| 00001000 | network operational | reset – unspecified | NSP |
| 00001001 | access operational | reset – user synchronization | NSU |
| 00001010 | network congestion | reset – network congestion | NSP |
| 00001011 | not obtainable [a] | reset – unspecified | NSP |
| 00001011 | not obtainable [a] | reset – undefined | undefined |
| 00001100 | unqualified | reset – unspecified | NSP |
| 00001100 | unqualified | reset – undefined | undefined |

NSU Network Service User

NSP Network Service Provider

[a] The need for this value is for further study.

**Recommendation Q.714**

# SIGNALLING CONNECTION CONTROL PART PROCEDURES

## 1 Introduction

### 1.1 *General characteristics of signalling connection control procedures*

#### 1.1.1 *Purpose*

This Recommendation describes the procedures performed by the Signalling Connection Control Part (SCCP) of Signalling System No. 7 to provide both connection-oriented and connectionless network services, and SCCP management services as defined in Recommendation Q.711. These procedures make use of the messages and information elements defined in Recommendation Q.712, whose formatting and coding aspects are specified in Recommendation Q.713.

#### 1.1.2 *Protocol classes*

The protocol used by the SCCP to provide network services is subdivided into four protocol classes, defined as follows:

- Class 0: Basic connectionless class
- Class 1: Sequenced (MTP) connectionless class
- Class 2: Basic connection-oriented class
- Class 3: Flow control connection-oriented class

The connectionless protocol classes provide those capabilities that are necessary to transfer one Network Service Data Unit (NSDU), (i.e., one user-to-user information block) in the user data field of a *Unitdata* message. The maximum length of a NSDU is restricted to X octets[1)], since segmenting and reassembly are not provided by protocol classes 0 and 1.

The connection-oriented protocol classes (protocol classes 2 and 3) provide segmenting and reassembly capabilities. If a Network Service Data Unit is longer than 255 octets, it is split into multiple segments at the originating node, prior to transfer in the "data" field of *Data* messages. Each segment is less than or equal to 255 octets. At the destination node, the NSDU is reassembled.

##### 1.1.2.1 *Protocol class 0*

Network Service Data Units passed by higher layers to the SCCP in the node of origin are delivered by the SCCP to higher layers in the destination node. They are transported independently of each other. Therefore, they may be delivered out-of-sequence. Thus, this protocol class corresponds to a pure connectionless network service.

##### 1.1.2.2 *Protocol class 1*

In protocol class 1, the features of class 0 are complemented by an additional feature (i.e., sequence control parameter associated with the N-UNITDATA request primitive) which allows the higher layer to indicate to the SCCP that a given stream of NSDUs have to be delivered in-sequence. The Signalling Link Selection (SLS) field is chosen by SCCP based on the value of the sequence control parameter. The SLS chosen for a stream of NSDUs with the same sequence control parameter will be identical. The SCCP will then encode the Signalling Link Selection (SLS) field in the routing label of messages relating to such NSDUs, so that their sequence is, under normal conditions, maintained by the signalling network as defined in Recommendation Q.704. Thus, this class corresponds to an enhanced connectionless service, where an additional sequencing feature is included.

---

[1)] Due to the ongoing studies on the SCCP called and calling party address, the maximum of this value needs further study. It is also noted that the transfer of up to 255 octets of user data is allowed when the SCCP called and calling party address do not include global title.

1.1.2.3 *Protocol class 2*

In protocol class 2, bidirectional transfer of NSDUs between the user of the SCCP in the node of origin and the user of the SCCP in the destination node is performed by setting up a temporary or permanent signalling connection. A number of signalling connections may be multiplexed onto the same signalling relation, as defined in Recommendation Q.704; such a multiplexing is performed by using a pair of reference numbers, referred to as "local reference numbers". Messages belonging to a given signalling connection will contain the same value of the SLS field to ensure sequencing as described in § 1.1.2.2. Thus, this protocol class corresponds to a simple connection-oriented network service, where SCCP flow control and missequence detection are not provided.

1.1.2.4 *Protocol class 3*

In protocol class 3, the features of protocol class 2 are complemented by the inclusion of flow control, with its associated capability of expedited data transfer. Moreover, an additional capability of detection of message loss or mis-sequencing is included; in such a circumstance, the signalling connection is reset and a corresponding notification is given by the SCCP to the higher layers.

1.1.3 *Signalling connections*

In all connection-oriented protocol classes, a signalling connection between the nodes of origin and destination may consist of:

- a single connection section, or
- a number of connection sections in tandem, which may belong to different interconnected signalling networks.

In the former case, the originating and destination nodes of the signalling connection coincide with the originating and destination nodes of a connection section. During the connection establishment phase, SCCP routing and relaying functions, as described in § 2 of this Recommendation, may be required at one or more intermediate nodes. Once the signalling connection has been established, though, SCCP functions are not required at intermediate nodes.

In the latter case, at any intermediate node where a message is received from a connection section and has to be sent on another connection section, the SCCP routing and relaying functions are involved during connection establishment. In addition, SCCP functions are required at intermediate nodes during Data Transfer and Connection Release to provide the association of connection sections.

1.1.4 *Compatibility and handling of unrecognized information*

1.1.4.1 *Rules for forward compatibility*

All implementations must recognize all messages in each protocol class offered, as indicated in Table 1/Q.713.

General rules for forward compatibility are specified in Recommendation Q.700.

1.1.4.2 *Handling of unrecognized messages or parameters*

Any message with unrecognized message type value should be discarded. Any unrecognized parameter within a message should be ignored. Notification to the originator of the message in these two cases is for further study.

1.2 *Overview of procedures for connection-oriented services*

1.2.1 *Connection establishment*

When the SCCP functions at the node of origin receive a request to establish a signalling connection, the "called party address" is analyzed to identify the node towards which a signalling connection should be established. The SCCP forwards a *Connection Request* (CR) message to that signalling point, using the MTP functions.

The SCCP in the node receiving the CR message via the MTP functions examines the "called party address" and one of the following actions takes place at the node:

a) If the "called party address" contained in the CR message corresponds to a user located in that signalling point and if the signalling connection may be established (i,e., establishment of a signalling connection is agreed to by the SCCP and local user), a *Connection Confirm* (CC) message is returned.

b) If the "called party address" does not correspond to a user at the signalling point, then information available in the message and at the node are examined to determine whether an association of two connection sections is required at that node.

   – If an association is required, then the SCCP establishes an (incoming) signalling connection section. Establishment of another (outgoing) connection section is initiated by sending a CR message towards the next node and this connection section is logically linked to the incoming connection section.

   – If coupling of the connection section is not required in this node, no incoming or outgoing connection section is established. A CR message is forwarded towards the next destination using the MTP routing function.

If the SCCP receives a CR message and either the SCCP or the SCCP user does not wish to establish the connection, then a *Connection Refused* (CREF) message is transferred on the incoming connection section.

On receipt of a CC message, the SCCP completes the set-up of a connection section. Furthermore, if coupling of two adjacent connection sections is needed, a further CC message is forwarded to the preceding node.

If no coupling of adjacent connection sections was needed during set-up in the forward direction, the CC message can be sent directly to the node of origin even if a number of intermediate SCCP nodes was passed in the forward direction. The OPC of the node of origin is transmitted within the "calling party address" Field.

When the CR and CC messages have been exchanged between all the involved nodes as above described, and the corresponding indications have been given to the higher layer functions in the nodes of origin and destination, then the signalling connection is established and transmission of messages may commence.

### 1.2.2 *Data transfer*

Transfer of each NSDU is performed by one or more *Data* (DT) messages; a *more-data* indication is used if the NSDU is to be split among more than one DT message. If protocol class 3 is used, then SCCP flow control is utilized over each connection section of the signalling connection. If, in such a protocol class, abnormal conditions are detected, then the appropriate actions are taken on the signalling connection (e.g., reset). Moreover in such a protocol class, expedited data may be sent using one *Expedited Data* message that bypasses the flow control procedures applying to *Data* messages.

A limited amount of data may also be transferred in the *Connection Request, Connection Refused* and *Connection Released* messages.

### 1.2.3 *Connection release*

When the signalling connection is terminated, a release sequence takes place by means of two messages called *Released* and *Release Complete* (RLC). The RLC message is normally sent in reaction to the receipt of a RLSD message.

## 1.3 *Overview of procedures for connectionless services*

### 1.3.1 *General*

When the SCCP functions at the node of origin receive from an SCCP user an NSDU to be transferred by the protocol class 0 or 1 connectionless service, the "called party address" and other relevant parameters, if required, are analyzed to identify the node towards which the message should be sent. The NSDU is then included as the "data" parameter in a *Unitdata* (UDT) message, which is sent towards the node using the MTP functions. Upon receipt of the UDT message, the SCCP functions at that node perform the routing analysis as described in § 2 of this Recommendation and, if the destination of the UDT message is a local user, deliver the NSDU to the local higher layer functions. If the "called party address" is not at that node, then the UDT message is forwarded to the next node. This process continues until the NSDU has reached the "called party address".

### 1.4 *Structure of the SCCP and contents of specification*

The basic structure of the SCCP appears in Figure 1/Q.714. It consists of four functional blocks as follows:

a) *SCCP connection-oriented control:* its purpose is to control the establishment and release of signalling connections and to provide for data transfer on signalling connections.

b) *SCCP connectionless control:* its purpose is to provide for the connectionless transfer of data units.

c) *SCCP management:* its purpose is to provide capabilities, in addition to the Signalling Route Management and flow control functions of the MTP, to handle the congestion or failure of either the SCCP user or the signalling route to the SCCP user.

d) *SCCP routing:* upon receipt of a message from the MTP or from functions a) or b) above, SCCP routing provides the necessary routing functions to either forward the message to the MTP for transfer, or pass the message to functions a) or b) above. A message whose "called party address" is a local user is passed to functions a or b, while one destined for a remote user is forwarded to the MTP for transfer to a distant SCCP user.

Section 2 of this specification describes the addressing and routing functions performed by the SCCP. Section 3 specifies the procedures for the connection-oriented services (protocol classes 2-3). Section 4 specifies the procedures for the connectionless services (protocol classes 0 and 1). Section 5 specifies the SCCP management procedures.

## 2 Addressing and routing

### 2.1 *SCCP addressing*

The "called and calling party addresses" contain the information necessary for the SCCP to determine an originating and destination node. In the case of the connection-oriented procedures, the addresses are the originating and destination points of the signalling connection, while in the case of the connectionless procedures, the addresses are the originating and destination points of the message.

When transferring connection-oriented or connectionless messages, two basic categories of addresses are distinguished by SCCP routing:

1) *Global Title* – A global title is an address, such as dialled-digits, which does not explicitly contain information that would allow routing in the signalling network, that is the translation function of the SCCP is required. This translation function could be performed on a distributed basis or on a centralized basis. The last case, where a request for translation is sent to a centralized data base, may be accomplished, for example, with transaction capabilities (TC). This matter is for further study.

   In case of an E.164-based global title with the nature of address indicator included, the sending sequence of address information will be the country code, followed by the national (significant) number. Within the destination signalling network, the address information may be the subscriber number or the national (significant) number, by choice of the value of nature of address indicator, as required by the administration concerned.

2) *DPC + SSN* – A Destination Point Code and Subsystem Number allows direct routing by the SCCP and MTP, that is, the translation function of the SCCP is not required.

### 2.2 *SCCP routing principles*

The SCCP routing control (SCRC) receives messages from the Message Transfer Part for routing and discrimination, after they have been received by the MTP from another node in the signalling network. SCRC also receives internal messages from SCCP connection-oriented control (SCOC) and connectionless control (SCLC) and performs any necessary routing functions (e.g., address translation) before passing them to the MTP for transport in the signalling network or back to the SCCP connection-oriented or connectionless control.

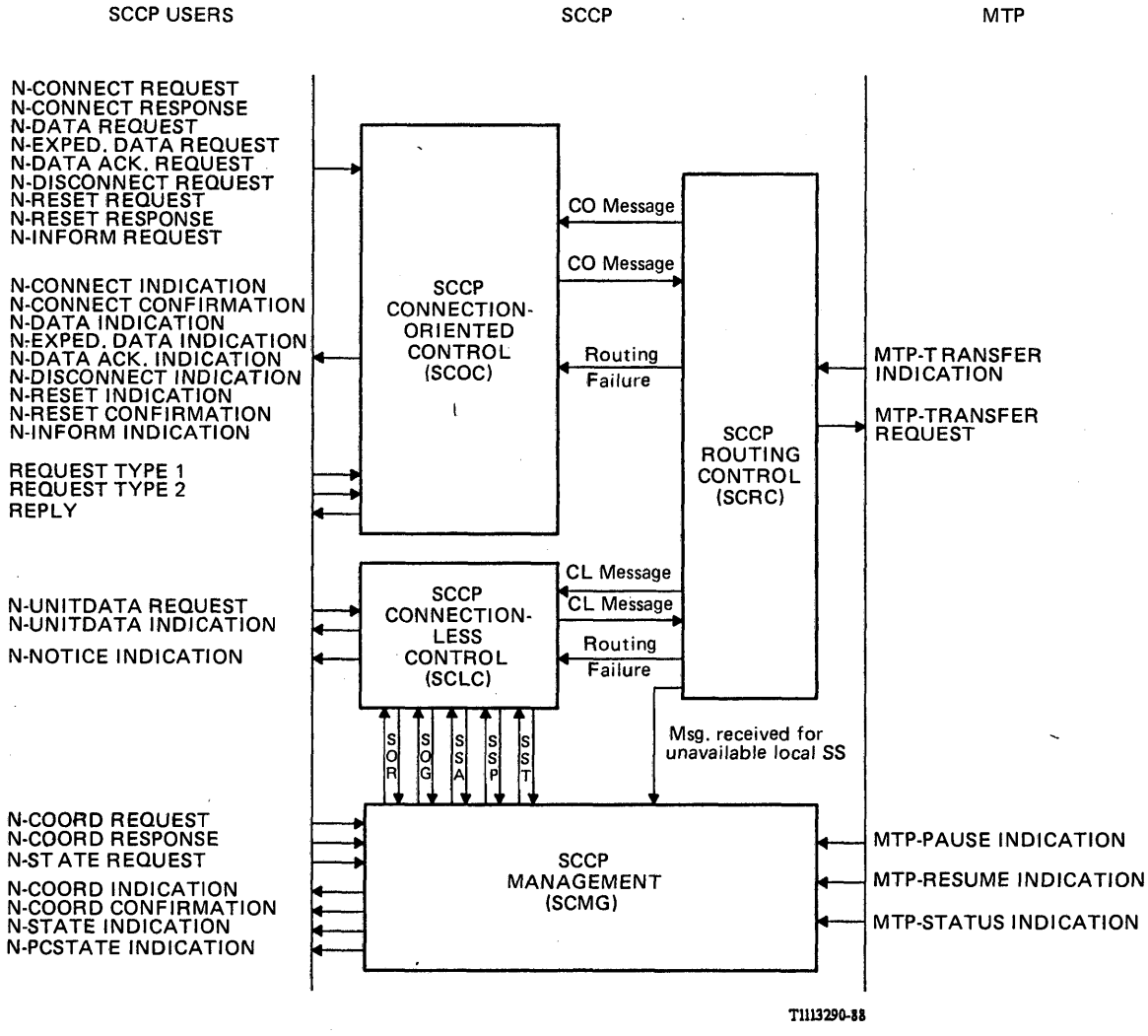



FIGURE 1/Q.714

**SCCP overview**

2.2.1 *Receipt of SCCP message transferred by the MTP*

A message transferred by the MTP that requires routing will include the "called party address" parameter giving information for routing the message. These messages currently include the *Connection Request* message and all types of connectionless messages. Other messages are passed to connection-oriented control for processing.

If the "called party address" parameter is used for routing, it can take the following information:

1) *Subsystem Number (SSN) only* – This indicates that the receiving SCCP is the termination point of the message. The SSN is used to determine the local subsystem.

2) *Global Title (GT) only* – This indicates that translation is required. Translation of the Global Title results in a new destination point code (DPC) for routing the message, and possibly a new SSN or GT or both in the "called party address".

3) *SSN + GT* – In this case, the address indicator information is used to determine whether the SSN or the GT should be used for routing and processing via items 1) or 2) above, respectively.

2.2.2 *Messages from connection-oriented or connectionless control to SCCP routing control*

Addressing information, indicating the destination of the message, is included with every internal message received from connection-oriented or connectionless control. For connectionless messages, this addressing information is obtained from the "called address" parameter associated with the N-UNITDATA REQUEST primitive. For *Connection-Request* messages received by SCCP routing, the addressing information is obtained from the "Called address" parameter associated with the N-CONNECT REQUEST primitive. For connection-oriented messages other than a *Connection Request* message, the addressing information (i.e., the DPC) is that associated with the connection section. The addressing information can take the following forms:

1) DPC

2) DPC + (SSN or GT or both)

3) GT

4) GT + SSN

The first form applies to connection-oriented messages except the *Connection Request* message. The last three forms apply to connectionless messages and to the *Connection Request* message.

2.2.2.1 *DPC present*

If the DPC is present in the addressing information, then the DPC is passed to the MTP using the MTP-TRANSFER request primitive and:

1) if no other addressing information is available, no "called party address" is provided in the message;

2) if a SSN or GT or both are available, this information is used in the "called party address" with an indication of which is to be used for routing.

If the DPC is the node itself, then the information is passed to the specified internal subsystem.

2.2.2.2 *Translation required*

If the DPC is not present, then a global title translation is required before the message can be sent out. Translation results in a DPC and possibly a new SSN or new GT or both. If the GT and/or SSN resulting from a global title translation is different from the GT and/or SSN which was previously included in the called party address, the newly produced GT and/or SSN replaces the existing one. The routing procedures then continue as per § 2.2.2.1

2.3 *SCCP routing*

The SCCP routing functions are based on information contained in the "called party address".

2.3.1 *Receipt of SCCP message transferred by the MTP*

One of the following actions is taken by SCCP routing upon receipt of a message from the Message Transfer Part. The message is received by the SCCP when the MTP invokes a MTP-TRANSFER INDICATION.

1) If the message is a connection-oriented message other than a *Connection Request* (CR) message, then SCCP routing passes the message to connection-oriented control.

2) If the routing indicator in the "called party address" does not indicate route on global title, then SCCP routing checks the status of the subsystem.

   a) If the subsystem is available, the message is passed, based on the message type, to either connection-oriented control or connectionless control.

   b) If the system is unavailable and:

      – the message is a connectionless message, then the message return procedure is initiated;

      – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

      In addition, if the subsystem is failed, SCCP management is notified that a message was received for a failed subsystem.

3) If the routing indicator in the "called party address" indicates route on global title, a translation of the global title must be performed.

   a) If the translation of the global title exists, and both the DPC and SSN are determined, then:

      i) if the DPC is the node itself, then the procedures in 2) above are followed;

      ii) if the DPC is not the node itself, the DPC and SSN are available, and the message is a connectionless message, then the MTP-TRANSFER REQUEST primitive is invoked;

      iii) if the DPC is not the node itself, the DPC and SSN are available, and the message is a connection-oriented message, then:

         – if an association of connection sections is required, the message is passed to connection-oriented control;

         – if no association of connection sections is required, the MTP-TRANSFER REQUEST primitive is invoked;

      iv) if the DPC is not the node itself, and the DPC and/or SSN are not available and

         – the message is a connectionless message, then the message return procedure is initiated;

         – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

   b) If the translation of the global title exists and only a DPC or DPC + new GT is determined, then:

      i) if the DPC is available, and the message is a connectionless message, then the MTP-TRANSFER REQUEST primitive is invoked;

      ii) if the DPC is available, and the message is a connection-oriented message, then:

         – if an association of the connection sections is required, then the message is passed to connection-oriented control;

         – if no association of the connection section is required, then the MTP-TRANSFER REQUEST primitive is invoked.

      iii) if the DPC is not available and

         – the message is a connectionless message, then the message return procedure is initiated;

         – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

   c) If the translation of the global title does not exist, and

      – the message is a connectionless message, then the message return procedure is initiated;

      – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

2.3.2 *Messages from connectionless or connection-oriented control to SCCP routing control*

One of the following actions is taken by SCCP routing upon receipt of a message from connectionless control or connection-oriented control.

1) If the message is a *Connection Request* message at an intermediate node (where connection sections are being associated), and:

   a) the DPC is available, then the MTP-TRANSFER REQUEST primitive is invoked;

   b) the DPC is not available, then the connection refusal procedure is initiated.

2) If the message is a connection-oriented message other than a *Connection Request* message, and:

   a) the DPC is available, then the MTP-TRANSFER REQUEST primitive is invoked;

   b) the DPC is not available, then the connection release procedure is initiated.

3) If the "Called address" in the primitive associated with a *Connection Request* or connectionless message includes a DPC, and:

   a) the DPC and SSN are available, then the MTP-TRANSFER REQUEST primitive is invoked;

   b) the DPC and/or SSN are not available, then:

      – for connectionless messages, the message return procedure is initiated;

      – for connection-oriented messages (CR messages), the connection refusal procedure is initiated.

   c) the DPC is the node itself, then the procedures in § 2.3.1, 2) above are followed.[2)]

4) If the "Called address" in the primitive associated with a *Connection Request* or connectionless message does not include a DPC, then a translation of the global title must be performed.

   a) If the translation of the global title exists, and both the DPC and SSN are determined, then:

      i) if the DPC is the node itself, then the procedures in § 2.3.1, 2), above are followed.[2)]

      ii) if the DPC is not the node itself and DPC and SSN are available, then the MTP-TRANSFER REQUEST primitive is invoked;

      iii) if the DPC is not the node itself, and the DPC and/or SSN are not available and:

         – the message is a connectionless message, then the message return procedure is initiated;

         – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

   b) If the translation of the global title exists and only a DPC or DPC + new GT is determined, then

      i) if the DPC is available, then the MTP-TRANSFER REQUEST primitive is invoked;

      ii) if the DPC is not available and:

         – the message is a connectionless message, then the message return procedure is initiated;

         – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

   c) If the translation of the global title does not exist, and:

      – the message is a connectionless message, then the message return procedure is initiated;

      – the message is a connection-oriented message (a CR message), then the connection refusal procedure is initiated.

---

[2)] The function of routing between local subsystems is implementation dependent.

### 2.4 *Routing failures*

The SCCP recognizes a number of reasons for failure in SCCP routing control. Examples of these reasons are:

1) translation does not exist for addresses of this nature;
2) translation does not exist for this specific address;
3) network/subsystem failure;
4) network/subsystem congestion, and
5) unequipped user.

The precise classification of the causes by which such failures are recognized is for further study.

When SCCP routing is unable to transfer a message due to the unavailability of a Point Code or Subsystem, one of above reasons is indicated in the *Connection Refused* message, the *Connection Released* message or the *Unitdata Service* message.

## 3 Connection-oriented procedures

### 3.1 *Connection establishment*

#### 3.1.1 *General*

The connection establishment procedures consist of the functions required to establish a temporary signalling connection between two users of the Signalling Connection Control Part.

The connection establishment procedures are initiated by a SCCP user by invoking the N-CONNECT request primitive.

The ISDN-UP may initiate an SCCP connection in the same way as any other user, but may also request the SCCP to initiate a connection and return the information to the ISDN-UP for transmission in a call set-up message.

The signalling connections between two users of the Signalling Connection Control Part, which are referred to by the "Called/Calling address" parameters in the N-CONNECT REQUEST primitive, may be realized by the establishment of one or more connection sections. The SCCP user is not aware of how the SCCP provides the signalling connection (e.g. by one or more than one connection sections).

The realization of a signalling connection between two SCCP users then can be described by the following components:

1) one or more connection sections;
2) an originating node, where the "Calling address" is located;
3) zero or more intermediate nodes, where, for this signalling connection, there is no distribution to a SCCP user; and
4) a destination node, where the "Called address" is located.

The *Connection Request* message and the *Connection Confirm* message are used to set up connection sections.

#### 3.1.2 *Local reference numbers*

During connection establishment both a source and destination local reference number are assigned independently to a connection section.

Source and destination local reference numbers are assigned at connection section set-up for a permanent connection section.

Once the destination reference number is known, it is a mandatory field for all messages transferred on that connection section.

Each node will select the local reference that will be used by the remote node as the destination local reference number field on a connection section for data transfer.

The local reference numbers remain unavailable for use on other connection sections until the connection section is released and the reference numbers are removed from their frozen state. See also § 3.3.2.

### 3.1.3 *Negotiation procedures*

#### 3.1.3.1 *Protocol class negotiation*

During connection establishment it is possible to negotiate the protocol class of a signalling connection between two SCCP users.

The N-CONNECT REQUEST primitive contains a parameter, the "Quality of service parameter set", with the preferred quality of service proposed by the SCCP user for the signalling connection.

The SCCP at the originating, intermediate and destination nodes may alter the protocol class on a signalling connection so that the quality of service assigned to the signalling connection is less restrictive (e.g., a protocol class 2 connection may be provided if a protocol class 3 connection is proposed). Information concerning the present proposed protocol class within the SCCP is carried in the *Connection Request* message and the assigned protocol class appears in the *Connection Confirm* message.

At the destination node the SCCP user is notified of the proposed protocol class using the N-CONNECT INDICATION primitive.

The protocol class of a signalling connection may also be altered by the Called SCCP user in the same manner (i.e. less restrictive) when invoking the N-CONNECT RESPONSE primitive.

The Calling SCCP user is informed of the quality of service selected on the signalling connection using the N-CONNECT CONFIRMATION primitive.

#### 3.1.3.2 *Flow control credit negotiation*

During connection establishment it is possible to negotiate the window size to be used on a signalling connection for the purpose of flow control. This window size remains fixed for the life of the signalling connection. The credit field in the CONNECTION REQUEST and CONNECTION CONFIRM messages is used to indicate the window size.

The N-CONNECT REQUEST primitive contains a parameter, the "Quality of service parameter set" with the preferred quality of service proposed by the SCCP user for the signalling connection.

The SCCP at the originating, intermediate and destination nodes may alter the window size on a signalling connection so that the quality of service assigned to the signalling connection is less restrictive (e.g., a smaller window size may be provided). Information concerning the present proposed window size within the SCCP is carried in the *Connection Request* message and the assigned window size appears in the *Connection Confirm* message.

At the destination node the SCCP user is notified of the proposed window size using the N-CONNECT indication primitive.

The window size of a signalling connection may also be altered by the Called SCCP user in the same manner (i.e. less restrictive) when invoking the N-CONNECT RESPONSE primitive.

The Calling SCCP user is informed of the quality of service selected on the signalling connection using the N-CONNECT confirm primitive.

### 3.1.4 *Actions at the origination node*

#### 3.1.4.1 *Initial actions*

The N-CONNECT REQUEST primitive is invoked by the SCCP user at the originating node to request the establishment of a signalling connection to the "Called address" contained in the primitive. The node determines if resources are available.

If resources are not available, then the connection refusal procedure is initiated.

If resources are available, then the following actions take place at the originating node:

1) A source local reference number and an SLS code are assigned to the connection section.
2) The "Called address" is associated with the connection section.
3) The proposed protocol class is determined for the connection section.

4) If the protocol class provides for flow control, then an initial credit is indicated in the *Connection Request* message.

5) The *Connection Request* message is then forwarded to the SCCP routing function for transfer.

6) A timer T(conn est) is started.

The ISDN-UP may request the SCCP to set up a SCCP signalling connection and return the information normally carried in a *Connection request* message to the ISDN-UP for transmission in a call set-up message.

When the ISDN-UP notifies the SCCP of the need for the connection, using the REQUEST Type 1 interface element, the SCCP determines if resources are available.

If resources are not available, then the connection refusal procedure is initiated. If resources are available, then the following actions take place at the origination node:

1) A source local reference number and an SLS code is assigned to the connection section.

2) An indication that the call request is from the ISDN-UP is associated with the connection section.

3) The proposed protocol class is determined for the connection section.

4) If the protocol class provides for flow control, then an initial credit is indicated.

5) The information that would normally be included in a Connection Request message is passed to the ISDN-UP for transfer using the REPLY interface element.

6) A timer T(conn est) is started.

#### 3.1.4.2 *Subsequent actions*

When an originating node receives a *Connection Confirm* message, the following actions are performed:

1) The protocol class and initial credit for flow control of the connection section are updated if necessary.

2) The SCCP user is informed of the successful establishment of the signalling connection using the N-CONNECT CONFIRMATION primitive.

3) The received local reference number is associated with the connection section.

4) The timer T(conn est) is stopped.

5) The inactivity control timers, T(ias) and T(iar), are started.

When the SCCP user at an origination node invokes the N-DISCONNECT REQUEST primitive, no action is taken prior to receipt of a *Connection Confirm* or a *Connection Refused* message or expiration of the connection establishment timer.

When an originating node receives a *Connection Refused* message, the connection refusal procedure is completed at the origination node (see § 3.2.3).

When the connection establishment timer at the origination node expires, the N-DISCONNECT INDICATION primitive is invoked, the resources associated with the connection section are released, and the local reference number is frozen.

### 3.1.5 *Actions at an intermediate node*

#### 3.1.5.1 *Initial actions*

When a *Connection Request* message is received at a node and the SCCP routing and discrimination function determines that the "called party address" is not a local SCCP user and that a coupling is required at this node, the intermediate node determines if resources are available to establish the connection section.

If resources are not available at the node, then the connection refusal procedure is initiated.

If resources are available at the node, then the following actions are performed:

1) A local reference number and an SLS code are assigned to the incoming connection section. (*Note* – As an implementation option, a local reference number may be assigned later upon reception of a *Connection Confirm* message.)
2) A connection section is set up to the remote node determined by SCCP Routing:
   - A local reference number and an SLS code are assigned to the outgoing connection section.
   - The protocol class is proposed.
   - An initial credit for flow control is assigned, if appropriate.
   - The *Connection Request* message is forwarded to the SCCP Routing with the same addressing information as found in the incoming *Connection Request* message.
   - The timer T(conn est) is started.
3) An association is made between the incoming and outgoing connection sections.

The ISDN-UP informs the SCCP that a connection request has been received using the REQUEST Type 2 interface element. The ISDN-UP passes the information contained in the ISDN-UP set-up message to the SCCP and indicates that a coupling is required at this node. The SCCP at the intermediate node then determines if resources are available to establish the connection section.

If resources are not available at the node, then the connection refusal procedure is initiated.

If resources are available at the node, then the following actions are performed:

1) A local reference number and an SLS code are assigned to the incoming connection section.
2) A local reference number and an SLS code is assigned to an outgoing connection section.
3) A protocol class is proposed.
4) An initial credit for flow control is assigned if appropriate.
5) An association is made between the incoming and outgoing connection sections.
6) The information that would normally be included in a conection request message is passed to the ISDN-UP for transfer in the REPLY interface element.
7) The timer T(conn est) is started.

3.1.5.2 *Subsequent actions*

When an intermediate node receives a *Connection Confirm* message, the following actions are performed:

1) The source local reference number in the *Connection Confirm* message is associated with the outgoing connection section.
2) The protocol class and credit for the connection section are assigned and identical to those found in the received *Connection Confirm* message.
3) A *Connection Confirm* message is transferred, using the SCCP routing function, to the originating node of the associated connection section. The protocol class and credit are identical to those indicated in the received *Connection Confirm* message.
4) The timer T(conn est) is stopped.
5) The inactivity control timers, T(ias) and T(iar), are started.

When an intermediate node receives a *Connection Refused* message, the connection refusal procedure is completed at that node (see § 3.2.2).

When the connection establishment timer expires at an intermediate node, the following actions are performed:

1) The resources associated with the connection are released.
2) The local reference number is frozen (see § 3.3.2).
3) If the connection section was established using a REQUEST interface element, then the N-DISCONNECT INDICATION primitive is invoked.
4) The connection refusal procedure is initiated on the associated connection section (see § 3.2.1).

### 3.1.6 *Actions at destination node*

#### 3.1.6.1 *Initial actions*

When a *Connection Request* message is received at a node, and the SCCP routing and discrimination function determines that the "called party address" is a local user, the destination node determines if resources are available to establish the connection section.

If resources are not available at the node, then the connection refusal procedure is initiated.

If the resources are available at the node, then the following actions are performed:

1) The protocol class is determined for the connection section. (*Note* – As an implementation option, a local reference number may also be assigned for the connection section.)
2) An initial credit for flow control is assigned if appropriate.
3) The node informs the SCCP user of a request to establish a connection using the N-CONNECT INDICATION primitive.

When the ISDN-UP informs the SCCP that a connection request has been received using the REQUEST Type 2 interface element, the ISDN-UP passes the information contained in the ISDN-UP set-up message to the SCCP, and informs the SCCP that the information is for a local user. The SCCP at the destination node determines if resources are available to establish the connection section.

If resources are not available at the node, then the connection refusal procedure is initiated.

If resources are available at the node, then the following actions are performed:

1) The protocol class is determined for the connection section.
2) An initial credit for flow control is assigned if appropriate.
3) The node informs the ISDN-UP of the request to establish a connection using the N-CONNECT INDICATION primitive.

#### 3.1.6.2 *Subsequent actions*

When a N-CONNECT RESPONSE primitive is invoked by the SCCP user at a destination node, the following actions are performed:

1) A local reference number and an SLS code are assigned to the incoming connection section.
2) The protocol class and credit are updated for the connection section if necessary.
3) A *Connection Confirm* message is transferred, using the SCCP routing function, to the originating node of the connection section.
4) The inactivity control timers, T(ias) and T(iar), are started.

## 3.2 *Connection refusal*

The purpose of the connection refusal procedure is to indicate to the Calling SCCP user function that the attempt to set up a signalling connection section was unsuccessful.

### 3.2.1 *Actions at node initiating connection refusal*

The connection refusal procedure is initiated by either the SCCP user or the SCCP itself:

1) The SCCP user at the destination node
   a) uses the N-DISCONNECT REQUEST (originator indicates "user initiated") after the SCCP has invoked an N-CONNECT indication primitive. This is the case when the SCCP at the destination node has received the connection request directly from a preceding SCCP.
   b) uses the refusal indicator in the REQUEST Type 2 interface element when the SCCP user has received the connection request embedded in a user part message.

2) The SCCP initiates connection refusal[3] (originator indicates "network initiated") due to:

   a) limited resources at an originating, intermediate or destination node, or

   b) expiration of the connection establishment timer at an originating or intermediate node.

Initiation of the connection refusal procedure by either the SCCP or the user results in the transfer of a *Connection Refused* message on the connection section. The refusal cause contains the value of the originator in the primitives; if the refusal procedure has been initiated by using the refusal indicator in the REQUEST Type 2 interface element, the refusal cause contains "SCCP user originated".

At the originating node, a connection refusal is initiated by invoking N-DISCONNECT INDICATION primitive.

If the connection refusal procedure is initiated at an intermediate node due to lack of resources, then a *Connection Refused* message is transferred on the incoming connection section.

If the connection refusal procedure is initiated at an intermediate node due to expiration of the connection establishment timer, then the connection release procedure is initiated on that connection section (see § 3.3.4.1) and a *Connection Refused* message is transferred on the associated connection section.

In either of the two above cases at an intermediate node, if the connection set-up was initiated using a REQUEST interface element, then the SCCP user is informed by invoking the N-DISCONNECT INDICATION primitive.

### 3.2.2 *Actions at intermediate node not initiating connection refusal*

When a *Connection Refused* message is received on a connection section, the following actions are performed:

1) The resources associated with the connection section are released and the timer T(conn est) is stopped[3].

2) If the connection was established using a REQUEST interface element, then the SCCP user is informed by invoking the N-DISCONNECT INDICATION primitive.

3) A *Connection Refused* message is transferred on the associated connection section.

4) The resources associated with the associated connection section are released.

### 3.2.3 *Actions at the origination node not initiating connection refusal*

When a *Connection Refused* message is received on a connection section, the following actions are performed:

1) The resources associated with the connection section are released and the timer T(conn est) is stopped[3].

2) The SCCP user is informed by invoking the N-DISCONNECT INDICATION primitive.

## 3.3 *Connection release*

### 3.3.1 *General*

The connection release procedures consist of the functions required to release a temporary signalling connection between two users of the Signalling Connection Control Part. Two messages are required to initiate and complete connection release: *Released* and *Release Complete.*

The release may be performed:

a) by either or both of the SCCP users to release an established connection.

b) by the SCCP to release an established connection.

All failures to maintain a connection are indicated in this way.

---

[3] If the reason for the refusal is "destination address unknown", then the maintenance function is alerted.

3.3.2 *Frozen reference*

The purpose of the frozen reference function is to prevent the initiation of incorrect procedures as a connection section due to receipt of a message, which is associated with a previously established connection section.

When a connection section is released, the local reference number associated with the connection section is not immediately available for reuse on another connection section. A mechanism should be chosen to sufficiently reduce the probability of erroneously associating a message with a connection section. This particular mechanism is implementation dependent.

3.3.3 *Actions at an end node initiating connection release*

3.3.3.1 *Initial actions*

When a connection release is initiated at an end node of a signalling connection, by the SCCP user invoking a N-DISCONNECT REQUEST primitive or by the node itself, the following actions are performed at the initiating node:

1) A *Released* message is transferred on the connection section.
2) A release timer T(rel) is started.
3) If the release was initiated by the SCCP, then a N-DISCONNECT INDICATION primitive is invoked.
4) The inactivity control timers, T(ias) and T(iar), if still running, are stopped.

3.3.3.2 *Subsequent actions*

The following actions are performed at the originating node on a connection section for which a *Released* message has been previously transferred:

1) When a *Release Complete* or *Released* message is received, the resources associated with the connection are released, the timer, T(rel), is stopped, and the local reference number is frozen.
2) When the release timer expires, a *Released* message is transferred on the connection section. The sending of the *Released* message is repeated every 4-15 seconds for an interval of up to one minute. At this point a maintenance function is alerted.

3.3.4 *Actions at intermediate node*

The connection release procedure is initiated at an intermediate node by the SCCP or by reception of a *Released* message on a connection section.

3.3.4.1 *Initial actions*

When a *Released* message is received on a connection section, the following actions then take place:

1) A *Release Complete* message is transferred on the connection section, the resources associated with the connection are released and the local reference number is frozen.
2) A *Released* message is transferred on the associated connection section; the reason is identical to the reason in the received message.
3) If the connection was established using a REQUEST interface element, then a N-DISCONNECT INDICATION primitive is invoked.
4) The release timer, T(rel), is started on the associated connection.
5) The inactivity control timers, T(ias) and T(iar), if still running, are stopped on both connection sections.

When the connection release procedure is initiated by the SCCP at the intermediate node during the data transfer phase, the following actions take place on both of the connection sections:

1) A *Released* message is transferred on the connection section.
2) If the connection section was established using an interface element, then a N-DISCONNECT INDICATION primitive is invoked.
3) The release timer, T(rel), is started.
4) The inactivity control timers, T(ias) and T(iar), if still running, are stopped on both connection sections.

3.3.4.2 *Subsequent actions*

The following actions are performed at an intermediate node during connection release:

1) When a *Release Complete* or *Released* message is received on a connection section, the resources associated with the connection are released, the timer T(rel) is stopped, and the local reference number is frozen.
2) When the release timer expires, a *Released* message is transferred on the connection section. The sending of the Released message is repeated every 4-15 seconds for an interval of up to one minute. At this point a maintenance function is alerted.

3.3.5 *Actions at an end node not initiating connection release*

When a *Released* message is received at an end node of a signalling connection, the following actions are performed on the connection section:

1) A *Release Complete* message is sent on the connection section.
2) The resources associated with the connection section are released, the SCCP user is informed that a release has occured by invoking the N-DISCONNECT INDICATION primitive, and the local reference number is frozen.
3) The inactivity control timers, T(ias) and T(iar), if still running, are stopped.

3.4 *Inactivity control*

The purpose of the inactivity control is to recover from:

1) loss of a *Connection Confirm* message during connections establishment, and
2) the unsignalled termination of a connection section during data transfer, and
3) a discrepancy in the connection data held at each end of a connection.

Two inactivity control timers, the receive inactivity control timer T(iar) and the send inactivity control timer T(ias), are required at each end of a connection section. The length of the receive inactivity timer must be longer than the length of the send inactivity timer.

When any message is sent on a connection section, the send inactivity control timer is reset.

When any message is sent on a connection section, the receive inactivity control timer is reset.

When the send inactivity timer, T(ias), expires, an *Inactivity Test* (IT) message is sent on the connection section.

The receiving SCCP checks the information contained in the IT message against the information held locally. If a discrepancy is detected, the following actions (Table 1/Q.714) are taken:

When the receive inactivity control timer, T(iar), expires, the connection release procedure is initiated on a temporary connection section and an OA&M function is alerted for a permanent connection section.

As an alternative to inactivity control timers in the SCCP, there is also the possibility of supervising a signalling connection by a SCCP user function.

TABLE 1/Q.714

| Discrepancy | Action |
|---|---|
| Source reference number | Release connection |
| Protocol class | Release connection |
| Sequencing/segmenting [a)] | Reset connection |
| Credit [a)] | Reset connection |

[a)] Does not apply to class 2 connection.

## 3.5 *Data transfer*

### 3.5.1 *General*

The purpose of data transfer is to provide the functions necessary to transfer user information on a temporary or permanent signalling connection.

#### 3.5.1.1 *Actions at the originating node*

The SCCP user at the originating node requests transfer of user data on a signalling connection by invoking the N-DATA REQUEST primitive.

The *Data* message is then generated, which must be transferred on the connection section. If flow control procedures apply to the connection section, these procedures must be enacted before the message can be forwarded on the connection section.

#### 3.5.1.2 *Actions at the intermediate node*

If a signalling connection consists of more than one connection section, then one or more intermediate nodes are involved in the transfer of *Data* messages on the signalling connection.

When a valid *Data* message is received on an incoming connection section at an intermediate node, the associated outgoing connection section is determined. The intermediate node then forwards the *Data* message to the associated outgoing connection section for transfer to the distant node. If flow control procedures apply to the connection sections, then the appropriate procedures must be enacted on both connection sections. On the incoming connection section, these procedures relate to the reception of a valid *Data* message and on the outgoing connection section, the procedures control the flow of *Data* messages on the connection section.

#### 3.5.1.3 *Actions at the destination node*

When the destination node receives a valid *Data* message, the SCCP user (i.e., the Called Party Address) is notified by invoking the N-DATA INDICATION primitive. If flow control procedures apply to the signalling connection, the flow control procedures relating to the reception of a valid *Data* message are enacted.

3.5.2 *Flow control*

3.5.2.1 *General*

The flow control procedures apply during data transfer only, and are used to control the flow of *Data* messages on each connection section.

The flow control procedures apply only to protocol class 3.

The reset procedure causes reinitialization of the flow control procedure.

The expedited data procedure is not affected by this flow control procedure.

3.5.2.2 *Sequence numbering*

For protocol class 3, for each direction of transmission on a connection section, the *Data* messages are sequentially numbered.

The sequence numbering scheme of the *Data* messages is performed modulo 128 on a connection section.

Upon initialization or reinitialization of a connection section, message send sequence numbers, P(S), are assigned to *Data* messages on a connection section beginning with P(S) equal to 0. Each subsequent *Data* message sequence number is obtained by incrementing the last assigned value by 1. The sequence numbering scheme assigns sequence numbers up to 127.

3.5.2.3 *Flow control window*

A separate window is defined, for each direction of transmission, on a connection section in order to control the number of *Data* messages authorized for transfer on a connection section. The window is an ordered set of W consecutive message send sequence numbers associated with the *Data* messages authorized for transfer on the connection section.

The lower window edge is the lowest sequence number in the window.

The sequence number of the first *Data* message not authorized for transfer on the connection is the value of the lower window edge plus W.

The maximum window size is set during connection establishment for temporary connection sections. For permanent connection sections, the window size is fixed at establishment. The maximum size cannot exceed 127.

Negotiation procedures during connection establishment allow for the negotiation of the window size.

3.5.2.4 *Flow control procedures*

3.5.2.4.1 *Transfer of Data messages*

If flow control procedures apply to a connection section, then all *Data* messages on the connection section contain a send sequence number, P(S), and a receive sequence number, P(R). The procedure for determining the send sequence number to be used in a *Data* message is described in § 3.5.2.2. The receive sequence number, P(R), is set equal to the value of the next send sequence number expected on the connection section and P(R) becomes the lower window edge of the receiving window.

An originating or intermediate node is authorized to transmit a *Data* message if the message send sequence number of the message is within the sending window. That is, if P(S) is greater than or equal to the lower window edge and less than the lower window edge plus W. When the send sequence number of a *Data* message is outside of the sending window, the node is not authorized to transmit the message.

3.5.2.4.2 *Transfer of Data Acknowledgement messages*

*Data Acknowledgement* messages may be sent when there are no *Data* messages to be transferred on a connection section[4].

[4] Further study is required to determine criterion to be used to decide when *Data Acknowledgement* messages are sent for cases other than the congestion situation described in this section.

When a node transfers a *Data Acknowledgement* message on a connection section, it is indicating that the node is ready to receive W *Data* messages within the window starting with the receive sequence number, P(R), found in the *Data Acknowledgement* message. That is, P(R) is the next send sequence number expected at the remote node on the connection section. Furthermore, P(R) also becomes the lower window edge of the receiving window.

A *Data Acknowledgement* message must be sent when a valid *Data* message, as per § 3.5.2.4.3 on P(S) and P(R), is received and P(S) is equal to the upper edge of the receiving window and there are no *Data* messages to be transferred on the connection section. Sending of *Data Acknowledgement* messages before having reached the upper edge of the receiving window is also allowed during normal operation.

*Data acknowledgement* messages may also be sent by a node encountering congestion on a connection section as described below:

Assuming nodes X and Y are the two ends of a connection section, the following procedures apply.

When a node (Y) experiences congestion on a connection section, it informs the remote node (X) using the *Data Acknowledgement* message with the credit set to zero.

Node (X) stops transferring *Data* messages on the connection section.

Node X updates the window on the connection section using the value of the receive sequence number, P(R), in the *Data Acknowledgement* message.

Node X begins transfer of *Data* message when it receives a *Data Acknowledgement* message with a credit field greater than zero or when a *Reset* message is received on a connection section for which a *Data Acknowledgement* message with a credit field equal to zero had previously been received.

Node X updates the window on the connection using the credit value. The credit value in a *Data Acknowledgement* message must either equal zero or equal the initial credit agreed to at connection establishment.

### 3.5.2.4.3 *Reception of a Data or Data Acknowledgement message*

When an intermediate or destination node receives a *Data* message, it performs the following test on the send sequence number, P(S), contained in the *Data* message:

1) If P(S) is the next send sequence number expected and is within the window, then the node accepts the *Data* message and increments by one the value of the next sequence number expected on the connection section.
2) If P(S) is not the next send sequence number expected, then the reset procedure is initiated on the connection section.
3) If P(S) is not within the window, then this is considered a local procedure error and the connection reset procedure is initiated.
4) If P(S) is not equal to 0 for the first *Data* message received after initialization or reinitialization of the connection section, this is considered a local procedure error and the connection reset procedure is initiated.

The message receive sequence number, P(R), is included in *Data*, and *Data Acknowledgement* messages. When a node receives a *Data* or *Data Acknowledgement* message on a connection section, the value of the receive sequence number, P(R), implies that the remote node has accepted at least all *Data* messages numbered up to and including P(R) – 1. That is, the next expected send sequence number at the remote node is P(R). The receive sequence number, P(R), contains information from the node sending the message, which authorizes the transfer of a limited number of *Data* messages on the connection section. When a node receives a *Data* or *Data Acknowledgement* message:

a) the receive sequence number, P(R), contained in the message becomes the lower window edge of the sending window:
    1) if the value of P(R) is greater than or equal to the last P(R) received by the node on that connection section, and also,
    2) if the value of the received P(R) is less than or equal to the P(S) of the next *Data* message to be transferred on that connection section;
b) the node initiates the reset procedure on the connection section if the receive sequence number, P(R), does not meet conditions 1) and 2).

### 3.5.3 *Segmenting and reassembly*

During the data transfer phase, the N-DATA REQUEST primitive is used to request transfer of octet-aligned data (NSDUs) on a signalling connection. NSDUs longer than 255 octets must be segmented before insertion into the "data" field of a *Data* message.

The more-data indicator (M-bit) is used to reassemble a NSDU that has been segmented for conveyance in multiple *Data* messages. The M-bit is set to 1 in all *Data* messages except the last message whose data field relates to a particular NSDU. In this way, the SCCP can reassemble the NSDU by combining the data fields of all *Data* messages with the M-bit set to 1 with the following *Data* message with the M-bit set to 0. The NSDU is then delivered to the SCCP user using the N-DATA INDICATION. *Data* messages in which the M-bit is set to 1 do not necessarily have the maximum length.

Segmentation and reassembly are not required if the length of the NSDU is less than or equal to 255 octets.

## 3.6 *Expedited data transfer*

### 3.6.1 *General*

The expedited data procedure applies only during the data transfer phase and is applicable to protocol class 3.

For the case of expedited data transfer, each message contains one NSDU, and no segmenting and reassembly is provided.

If an *Expedited Data* or *Expedited Data Acknowledgement* message is lost, then subsequent *Expedited Data* messages cannot be forwarded on the connection section.

### 3.6.2 *Actions at the originating node*

The expedited data transfer procedure is initiated by the user of the SCCP using the N-EXPEDITED--DATA REQUEST primitive, which contains up to 32 octets of user data.

When the SCCP user invokes the N-EXPEDITED-DATA REQUEST primitive, an *Expedited Data* message with up to 32 octets of user data is transferred on the connection section once *all* previous *Expedited Data* messages for the connection section have been acknowledged.

### 3.6.3 *Actions at intermediate node*

Upon receiving a valid *Expedited Data* message, an intermediate node confirms this message by transferring an *Expedited Data Acknowledgement* message on the incoming connection section. Withholding of the *Expedited Data Acknowledgement* message is a means of providing flow control of *Expedited Data* messages.

If a node receives another *Expedited Data* message on the incoming connection section before sending the *Expedited Data Acknowledgement* message, then the node will discard the subsequent message and reset the incoming connection section.

The intermediate node determines the associated outgoing connection section. An *Expedited Data* message is then transferred on the associated outgoing connection section, once *all* previous *Expedited Data* messages on that connection section have been acknowledged.

The *Expedited Data Acknowledgement* message must be sent before acknowledging subsequent *Data* or *Expedited Data* messages received on the incoming connection section.

### 3.6.4 *Actions at destination node*

The destination node of the connection section confirms a valid *Expedited Data* message by transferring an *Expedited Data Acknowledgement* message on the connection section. Withholding of the *Expedited Data Acknowledgement* message is a means of providing flow control of *Expedited Data* messages.

If a node receives another *Expedited Data* message on a connection section before sending the *Expedited Data Acknowledgement* message, then the node will discard the subsequent message and reset the connection section.

The destination node then invokes the N-EXPEDITED DATA INDICATION primitive.

The N-EXPEDITED-DATA INDICATION must be issued to the SCCP user at destination node before N-DATA or N-EXPEDITED-DATA indications resulting from any subsequently issued N-DATA or N-EXPEDITED-DATA requests at the originating node of that signalling connection. The initiation of the *Expedited Data Acknowledgement* message is implementation dependent.

## 3.7 *Reset*

### 3.7.1 *General*

The purpose of the reset procedure is to reinitialize a connection section. It is applicable only to protocol class 3. It is noted that the time sequence of the primitives in the reset procedure may be varied as long as it is consistent with Recommendation X.213.

For a connection reset initiated by the SCCP, Data or Expedited Data messages should not be transferred on the connection section prior to the completion of the reset procedure.

### 3.7.2 *Action at the initiating node*

#### 3.7.2.1 *Initial actions*

When a connection reset is initiated, by the SCCP user invoking a N-RESET REQUEST primitive or by the node itself, the following actions are performed at the initiating node:

1) A *Reset Request* message is transferred on the connection section.
2) The send sequence number, P(S), for the next *Data* message is set to 0. The lower window edge is set to 0. The window size is reset to the initial credit value.
3) The SCCP user is informed that a reset has taken place by:
   - invoking the N-RESET INDICATION primitive if the reset is network originated.
4) The reset timer T (reset) is started.

#### 3.7.2.2 *Subsequent actions*

The following actions are performed at the initiating node on a connection section for which a *Reset Request* message has been previously transferred:

1) When a *Data, Data Acknowledgement, Expedited Data,* or *Expedited Data Acknowledgement* message is received, the message is discarded. When an N-DATA REQUEST or N-EXPEDITED DATA REQUEST primitive is received, the primitive is discarded or stored up to the completion of the reset procedure. The choice between these two is implementation dependent.
2) When the reset timer expires, the connection release procedure is initiated on a temporary connection section and maintenance functions are alerted for a permanent connection section.
3) When a *Reset Confirm* or a *Reset Request* message is received on the connection section, the reset is completed provided the SCCP has previously received an N-RESET REQUEST or RESPONSE primitive from the SCCP user and, therefore, data transfer is resumed and the timer T(reset) is stopped. The SCCP user is informed that the reset is completed by invoking the N-RESET CONFIRMATION primitive.
4) When a *Released* message is received on a temporary connection section, the release procedure is initiated and the timer, T (reset), is stopped.

### 3.7.3 *Actions at the intermediate node*

#### 3.7.3.1 *Initial actions*

The connection reset procedure is initiated at the intermediate node either by the SCCP at the node itself or by the reception of a *Reset Request* message.

When a *Reset Request* message is received on a connection section, the following actions take place:

1) A *Reset Confirm* message is transferred on the connection section.

2) A *Reset Request* message is transferred on the associated connection section; the reason for reset is identical to the reason in the *Reset Request* message.

3) On both the connection section and the associated connection section, the send sequence number, P(S), for the next *Data* message to be transmitted is set to 0 and the lower window edge is set to 0. The window size is reset to the initial credit value on both connection sections.

4) The data transfer procedure is initiated on the connection section.

5) The reset timer, T (reset), is started on the associated connection section.

When the connection reset procedure is initiated by the SCCP at the intermediate node, the following actions take place on both of the connection sections:

1) A *Reset Request* message is transferred.

2) The send sequence number, P(S), for the next *Data* message is set to 0. The lower window edge is set to 0. The window size is reset to the initial credit value.

3) The reset timer T (reset) is started.

#### 3.7.3.2 *Subsequent actions*

If the connection reset was initiated by reception of a *Reset Request* message on a connection section, then the following actions are performed after initial actions are completed:

1) When a *Data, Data Acknowledgement, Expedited Data, Expedited Data Acknowledgement* message is received on the associated connection section, the message is discarded.

2) When the reset timer expires on the associated connection section, the connection release procedure is initiated on both temporary connection sections and the maintenance function is alerted on an associated permanent connection section.

3) When a *Released* message is received on a temporary connection section, the connection release procedure is initiated on both connection sections and the timer, T (reset), is stopped.

4) When a *Reset Confirm* or *Reset Request* message is received on the associated connection section, the data transfer procedure is resumed and the timer, T (reset), is stopped.

If the connection reset was initiated by the SCCP at the intermediate node, then the following actions are performed once the initial actions are completed:

1) When a *Data, Data Acknowledgement, Expedited Data,* or *Expedited Data Acknowledgement* message is received on either connection section, the message is discarded.

2) When the reset timer expires on a temporary connection section, the connection release procedure is initiated on both connection sections, and on a permanent connection section a maintenance function is alerted.

3) When a *Released* message is received on a temporary connection section, the connection release procedure is initiated on both connection sections and the timer, T (reset), is stopped .

4) When a *Reset Confirm* or *Reset Request* message is received on a connection section, data transfer is resumed on that connection and the timer, T (reset), is stopped.

3.7.4 *Actions at the destination node*

When a *Reset Request* message is received at a node, the following actions are performed on the connection section:

1) The send sequence number, P(S), for the next *Data* message is set to 0, the lower window edge is set to 0. The window size is reset to the initial credit value.
2) The SCCP user is informed that a reset has occurred by invoking the N-RESET INDICATION primitive.
3) A *Reset Confirm* message is transferred on the connection section after an N-RESET RESPONSE or REQUEST primitive is invoked by the user.
4) An N-RESET CONFIRMATION primitive is invoked to inform the SCCP user that the reset is completed and the data transfer can be resumed.

3.7.5 *Handling of messages during the reset procedures*

Once the reset procedure is initiated, the following actions are taken with respect to *Data* messages:

- those that have been transmitted, but for which an acknowledgement has not been received, are discarded, and
- those that have not been transmitted, but are contained in an M-bit sequence for which some *Data* messages have been transmitted, are discarded,
- those *Data* messages that have been received, but which do not constitute an entire M-bit sequence, are discarded.

3.8 *Restart*

3.8.1 *General*

The purpose of the restart procedure is to provide a recovery mechanism for signalling connection sections in the event of a node failure.

3.8.2 *Actions at the recovered node*

3.8.2.1 *Initial actions*

When a node recovers from its failure, the following actions are performed:

1) A guard timer, T(guard)[5], is started.
2) If the recovered node has knowledge about the local reference numbers in use before failure, then the normal procedures for temporary signalling connections are resumed with the assumption that the local reference numbers which were in use before the node failure are not assigned at least during T(guard).
3) An OA&M function is informed for the re-establishment of permanent signalling connections.

3.8.2.2 *Subsequent actions*

The following actions are performed at the recovered node, on every temporary signalling connection section if the node does not know the local reference numbers in use before failure, or only on the temporary signalling connection sections in operation before failure if the node has such knowledge:

a) Before the guard timer, T(guard), expires:
   1) When a *Released* message is received with both source and destination local reference numbers, a *Release Complete* message, with reversed local reference numbers, is returned to the originating point code.
   2) Any other connection-oriented messages received are discarded.
b) When the guard timer, T(guard), expires, normal procedures are resumed.

[5] The guard timer must be large enough, so that all the non-failed far end nodes can detect the failure and can safely release the affected temporary signalling connection sections. This implies T(guard) > T(iar) + T(rel).

3.8.3 *Actions at the non-failed far end node*

The inactivity control procedure, described in § 3.4, is used by the non-failed far end node to recover from the unsignalled termination of a connection section during data transfer.

3.9 *Permanent signalling connections*

Permanent signalling connections are set up administratively and connection establishment procedures and connection release procedures are not initiated by the SCCP user.

Permanent signalling connections are realized using one or more connection sections.

A permanent signalling connection is either in the data transfer phase or the reset phase. Therefore, all procedures relating to the data transfer phase for connection-oriented protocol classes and the reset procedures are applicable to permanent signalling connections.

3.10 *Abnormalities*

3.10.1 *General*

Errors can be classified into the three categories listed below. Examples of each category are included for clarification:

1) *Syntax errors* – This type of error occurs when a node receives a message that does not conform to the format specifications of the SCCP. Examples of syntax errors are:
   - reception of message with an invalid message type code, and
   - reception of a message with an unassigned local reference number.
2) *Logical errors* – This type of error occurs when a node receives a message that is not an acceptable input to the current state of the connection section, or whose value of P(S) or P(R) is invalid. Examples of logical errors are:
   - reception of an acknowledgement message when the corresponding request message has not been sent,
   - reception of a *Data* message whose data field length exceeds the maximum data field permitted on the connection section,
   - reception of a second *Expedited Data* message before an *Expedited Data Acknowledgement* message has been sent, and
   - reception of message whose value of P(R) is not greater than or equal to the last P(R) received and is not less than or equal to the next value of P(S) to be transmitted.
3) *Transmission errors* – This type of error occurs when a message is lost or delayed. Examples of transmission errors are:
   - expiration of a timer before reception of the appropriate acknowledgement message.

3.10.2 *Action tables*

The action tables found in Recommendation Q.714, Annex B, include information, in addition to that found in the text of Recommendation Q.714, regarding the actions to be performed upon receipt of a message. In particular, these tables are helpful in determining the actions to be performed upon receipt of a message resulting in a logical error.

3.10.3 *Actions upon the reception of an ERR message*

Upon the reception of a *Protocol Data Unit Error* (ERR) message at a node, the following actions are performed on the connection section for error causes other than "service class mismatch":

1) The resources associated with the connection are released.
2) The local reference number is frozen (see § 3.3.2).

Upon the reception of a *Protocol Data Unit Error* (ERR) message at a node with the error cause "service class mismatch", the connection release procedure is initiated by the SCCP at that node (see § 3.3).

## 4 Connectionless procedures

The connectionless procedures allow a user of the SCCP to request transfer of up to X octets[6] of user data without first requesting establishment of a signalling connection.

The N-UNITDATA REQUEST and INDICATION primitives are used by the user of the SCCP to request transfer of user data by the SCCP and for the SCCP to indicate delivery of user data to the destination user. Parameters associated with the N-UNITDATA REQUEST primitive must contain all information necessary for the SCCP to deliver the user data to the destination.

Transfer of the user data is accomplished by including the user data in *Unitdata* messages.

The user of the SCCP should ensure that the total length of the user data and the SCCP address information does not exceed the total permissible length of the SCCP Unitdata message.

If user data of excessive length is presented by the user of the SCCP, the SCCP should not transmit a part of it to the remote user of the SCCP.

Whether or not the local SCCP user should be informed by the SCCP is implementation dependent.

When the user of the SCCP requests transfer of user data by issuing a N-UNITDATA REQUEST primitive, there are two classes of service that can be provided by the SCCP, protocol classes 0 and 1. These protocol classes are distinguished by their message sequencing characteristics.

When the user of the SCCP requests transfer of several messages by issuing multiple N-UNITDATA REQUEST primitives, the probability of these messages being received in sequence at the "Called address" depends on the protocol class designated in the request primitives. For protocol class 0 the sequence control parameter is not included in the N-UNITDATA REQUEST primitive and the SCCP may generate a different SLS for each of these messages. For protocol class 1 the sequence control parameter is included in the N-UNITDATA REQUEST primitive and, if the parameter is the same in each request primitive, then the SCCP will generate the same SLS for these messages.

The Message Transfer Part retains message sequencing for those messages with the same SLS field. The Signalling Connection Control Part relies on the services of the MTP for transfer of SCCP messages. Based on the characteristics of the MTP, the protocol class 1 service may be used in such a way that it provides a quality of service that has a lower probability of out-of-sequence messages than that provided by protocol class 0.

### 4.1 *Data transfer*

The N-UNITDATA REQUEST primitive is invoked by the SCCP user at an originating node to request connectionless data transfer service. The connectionless data transfer service is also used to transport SCCP management messages, which are transferred in the "data" field of *Unitdata* messages.

The *Unitdata* message is then transferred, using SCCP and MTP routing functions, to the "Called address" indicated in the UNITDATA REQUEST primitive.

SCCP routing and relaying functions may be required at intermediate nodes, since complete translation and routing tables for all addresses are not required at every node.

When the *Unitdata* message cannot be transferred to its destination, the message return function is initiated.

The SCCP uses the services of the MTP and the MTP may, under severe network conditions, discard messages. Therefore, the user of the SCCP may not always be informed of non-delivery of user data. The MTP notifies the SCCP of unavailable signalling points using the MTP-STOP INDICATION and of congested signalling points using the MTP-PAUSE INDICATION. The SCCP then informs its users.

When a *Unitdata* message is received at the destination node, a N-UNITDATA INDICATION primitive is invoked except for the SCCP management messages. The SCCP management (SCMG) messages are passed to the SCMG entity instead.

---

[6] Due to the ongoing studies on the SCCP called and calling party address, the maximum of this value needs further study. It is also noted that the transfer of up to 255 octets of user data is allowed when the SCCP called and calling party address do not include global title.

### 4.2 *Message return*

The purpose of message return is to discard or return messages which encounter routing failure and cannot be delivered to their final destination.

The message return procedure is initiated if SCCP routing is unable to transfer a *Unitdata* or *Unitdata Service* message. The procedure may be initiated, for example, as a result of insufficient translation information or the inaccessibility of a subsystem or point code. Specific reasons are enumerated in § 2.3.

a) If the message is a *Unitdata* message, and
   - the option field is set to return message on error, then a *Unitdata Service* message is transferred to the "calling party address". (If the message is originated locally, then a N-NOTICE INDICATION primitive is invoked.)
   - the option field is not set to return on error, then the message is discarded.

b) If the undeliverable message is a *Unitdata Service* message, it is discarded.

The user "data" field of the *Unitdata* message and the reason for return are included in the *Unitdata Service* message.

When a *Unitdata Service* message is received at the destination node, a N-NOTICE INDICATION primitive is invoked.

### 4.3 *Syntax error*

This type of error occurs when a node receives a message that does not conform to the format specifications of the SCCP. Examples of syntax errors are:

- unreasonable pointer value (e.g., points beyond the end of the message);
- mismatch between message type and protocol class parameters; and
- inconsistent address indicator and address contents.

When syntax error is detected for a connectionless message, the message is discarded. Checking for syntax errors beyond the processing required for the SCCP connectionless message routing is not mandatory.

## 5 SCCP management procedures

### 5.1 *General*

The purpose of SCCP management is to provide procedures to maintain network performance by rerouting or throttling traffic in the event of failure or congestion in the network.

Although SCCP management has its own subsystem number, the procedures in this section does not apply to it.

SCCP management is organized into two subfunctions: signalling point status management and subsystem status management. Signalling point status management and subsystem status management allow SCCP management to use information concerning the accessibility of signalling points and subsystems, respectively, to permit the network to adjust to failure, recovery and congestion.

SCCP management procedures rely on:

1) failure, recovery, and congestion information provided in the MTP-PAUSE INDICATION, MTP-RESUME INDICATION and MTP-STATUS INDICATION primitives; and
2) subsystem failure, recovery and congestion information received in SCCP management messages[7].

SCCP management information is currently defined to be transferred using SCCP connectionless service with no return on error requested. Formats of these messages appear in Recommendation Q.713.

---

[7] Subsystem congestion control is for further study.

The information pertaining to both single and replicated nodes or subsystems is used for SCCP management purposes. This allows "called party addresses" that are specified in the form of a global title to be translated to different point codes and/or subsystem numbers depending on network or subsystem status.

Replicated nodes or subsystems may relate to their replicates in one of several ways. ("Replicate" is a term meaning one of a set of "multiple copies". A node of subsystem which is not replicated is termed "solitary".)

One mode uses a replicate in a dominant role. Traffic is split among several nodes/subsystems. Under normal conditions, each portion of the traffic is routed to a preferred, or "primary", node/subsystem. When the primary node/subsystem is inaccessible, this traffic is routed to a "backup" node/subsystem . When the primary node/subsystem recovers, it reassumes its normal traffic load.

A second mode uses a replicate in a replacement role. Consider two replicates, A and B, which are "alternatives". When A becomes inaccessible, its traffic is routed to B; but when A recovers, the traffic is not moved back to A. It is only when B becomes inaccessible that traffic is shifted back to A. In addition, other modes are possible.

The current SCCP management procedures are designed to manage solitary nodes/subsystems, and replicated nodes/subsystems which operate in a dominant mode and for which any given primary node/subsystem has only one backup (i.e., duplicated nodes/subsystems). Management procedures for nodes/subsystems which operate in a mode other than the dominant mode and which have more than one backup are for further study.

SCCP management procedures utilize the concept of a "concerned" subsystem or signalling point. In this context, a "concerned" entity means an entity with an immediate need to be informed of a particular signalling point/subsystem status change, independently of whether SCCP communication is in progress between the "concerned" entity and the affected entity with the status change[8)].

In some situations, the number of concerned subsystem or signalling points for a given subsystem may be zero. In this case, when the subsystem fails, or becomes unavailable, no broadcast of the subsystem prohibited message is performed. Instead, the response method is used to return the subsystem prohibited message. Similarly, no broadcast of the subsystem allowed message is performed for that given subsystem when it recovers. The response method is again used to return a subsystem allowed message in reply to a subsystem status test.

The signalling point prohibited, signalling point allowed and signalling point congested procedures, specified in §§ 5.2.2, 5.2.3 and 5.2.4 respectively, deal with the accessibility of a signalling point.

The subsystem prohibited and subsystem allowed procedures, detailed in §§ 5.3.2 and 5.3.3 respectively, deal with the accessibility of a subsystem.

An audit procedure to ensure that necessary subsystem management information is always available is specified in the subsystem status test procedure in § 5.3.4.

A subsystem may request to go out of service using the coordinated state change control procedure specified in § 5.3.5.

Local subsystems are informed of any related subsystem status by the local broadcast procedure specified in § 5.3.6.

Concerned signalling points are informed of any related subsystem status by the broadcast procedure specified in § 5.3.7.

## 5.2 *Signalling point status management*

### 5.2.1 *General*

Signalling point status management updates translation and status based on the information of network failure, recovery, or congestion provided by the MTP-PAUSE INDICATION, MTP-RESUME INDICATION, or MTP-STATUS INDICATION primitives. This allows alternative routing to backup signalling points and/or backup subsystems.

---

[8)] Further explicit definition of "concerned" subsystems or signalling points would be network/architecture/application dependent.

5.2.2 *Signalling point prohibited*

When SCCP management receives a MTP-PAUSE INDICATION relating to a destination that become inaccessible, SCCP management:

1) marks the translation as appropriate:
   - "translate to backup node" if that signalling point has a backup;
   - "translate to backup subsystem" for each subsystem at that signalling point for which a backup subsystem exists.
2) marks as "prohibited" the status of that signalling point and of each subsystem at that signalling point.
3) discontinues any subsystem status tests (§ 5.3.4) it may be conducting to any subsystems at that signalling point.
4) initiates a local broadcast (§ 5.3.6) of "User-out-of-service" information for each subsystem at that signalling point.
5) initiates a local broadcast (§ 5.3.6) of "signalling point inaccessible" information for that signalling point.

5.2.3 *Signalling point allowed*

When SCCP management receives a MTP-RESUME INDICATION relating to a destination that becomes accessible, SCCP management:

1) resets the congestion level of that signalling point.
2) marks the translation as appropriate:
   - "translate to primary node" if that signalling point has a backup.
3) marks as "allowed" the status of that signalling point.
4) initiates the subsystem status test procedure (§ 5.3.4) with affected subsystems at that signalling point.
5) initiates a local broadcast (§ 5.3.6) of "signalling point inaccessible" information for that signalling point.

5.2.4 *Signalling point congested*

When SCCP management receives a MTP-status indication relating to signalling network congestion to a signalling point, SCCP management:

1) updates that signalling point status to reflect the congestion.
2) initiates a local broadcast (§ 5.3.6) of "signalling point congested" information for that signalling point.

5.3 *Subsystem status management*

5.3.1 *General*

Subsystem status management updates translation and status based on the information of failure, withdrawal, congestion[9], and recovery of subsystems. This allows alternative routing to backup systems, if appropriate. Local users are informed of the status of their backup subsystems.

5.3.2 *Subsystem prohibited*

5.3.2.1 *Receipt of messages for a prohibited subsystem*

If SCCP routing control receives a message, whether originated locally or not, for a prohibited local system, SCCP routing control invokes subsystem prohibited control. A *Subsystem-Prohibited* message is sent to the originating signalling point if the originating subsystem is not local (the OPC is a parameter in the MTP-TRANSFER INDICATION primitive). The action, if any, to be taken, if the originating subsystem is local, is for further study.

---

[9] Subsystem congestion control is for further study.

5.3.2.2 *Receipt of Subsystem-Prohibited message or N-STATE REQUEST primitive or local user failed*

Under one of the following conditions:

a) SCCP management receives a *Subsystem-Prohibited* message about a subsystem marked allowed, or

b) a N-STATE REQUEST primitive with "User-out-of-service" information is invoked by a subsystem marked allowed, or

c) SCCP management detects that a local subsystem has failed,

then SCCP management does the following:

1) marks the translation as appropriate:
   - "translate to backup subsystem" if a backup subsystem exists for the prohibited subsystem.
2) marks as "prohibited" the status of that subsystem.
3) initiates a local broadcast (§ 5.3.6) of "User-out-of-service" information for the prohibited subsystem.
4) initiates the subsystem status test procedure (§ 5.3.4) if the prohibited subsystem is not local.
5) forwards the information throughout the network by initiating a broadcast (§ 5.3.7) of *Subsystem-Prohibited* messages to concerned signalling points.
6) cancels "ignore subsystem status test" and the associated timer if they are in progress and if the newly prohibited subsystem resides at the local node.

5.3.3 *Subsystem allowed*

Under one of the following conditions:

a) SCCP management receives a *Subsystem-Allowed* message about a subsystem marked prohibited, or

b) a N-STATE REQUEST primitive with "User-in-Service" information is invoked by a subsystem marked prohibited,

then SCCP management does the following:

1) marks the translation as appropriate:
   - "translate to primary subsystem" if that subsystem is duplicated and the primary subsystem is allowed;
   - "translate to backup subsystem" if that subsystem is duplicated and the primary subsystem is prohibited.
2) marks as "allowed" the status of that subsystem.
3) initiates as a local broadcast (§ 5.3.6) of "User-in-service" information for the allowed subsystem.
4) discontinues the subsystem status test relating to that subsystem if such a test was in progress.
5) forwards the information throughout the network by initiating a broadcast (§ 5.3.7) of *Subsystem-Allowed* messages to concerned signalling points.

5.3.4 *Subsystem status test*

5.3.4.1 *General*

The subsystem status test procedure is an audit procedure to verify the status of a subsystem marked prohibited.

5.3.4.2 *Actions at the initiating node*

A subsystem status test is initiated when:

a) a *Subsystem-Prohibited* message is received (§ 5.3.2.2), or

b) a MTP-RESUME INDICATION primitive for a previously inaccessible signalling point is invoked (§ 5.2.3).

A subsystem status test associated with a failed subsystem is commenced by starting a timer (stat.info) and marking a test in progress. No further actions are taken until the timer expires.

Upon expiration of the timer, a *Subsystem-Status-Test* message is sent to SCCP management at the node of the failed subsystem and the timer is reset.

The cycle continues until the test is terminated by another SCCP management function at that node. Termination of the test causes the timer and the test mark to be cancelled.

#### 5.3.4.3 *Actions at the receiving node*

When SCCP management receives a *Subsystem-Status-Test* message and there is no "ignore subsystem status test" in progress, it checks the status of the named subsystem. If the subsystem is allowed, a *Subsystem-Allowed* message is sent to the SCCP management at the node conducting the test. If the subsystem is prohibited, no reply is sent.

### 5.3.5 *Coordinated state change*

#### 5.3.5.1 *General*

A duplicated subsystem may be withdrawn from service without degrading the performance of the network by using the coordinated state change procedure described below when its backup is not local. The procedure, if any, to be specified in case the primary and the backup subsystems are co-located, is for further study.

#### 5.3.5.2 *Actions at the requesting node*

When a duplicated subsystem wishes to go out of service, it invokes a N-COORD REQUEST primitive. SCCP management at that node sends a *Subsystem-Out-of-Service-Request* message to the backup system, sets a timer (coord.chg) and marks the subsystem as "waiting for grant".

Arrival of a *Subsystem-Out-of-Service-Grant* message at the requesting SCCP management causes the timer (coord.chg) to be cancelled, the "waiting for grant" state to be cancelled, and a N-COORD CONFIRMATION primitive to be invoked to the requesting subsystem. *Subsystem-Prohibited* messages are broadcast (§ 5.3.7) to concerned signalling points.

In addition, an "ignore subsystem status test" timer is started and the requesting subsystem is marked as "ignore subsystem status test". Subsystem status tests are ignored until the "ignore subsystem status test" timer expires or the marked subsystem invokes a N-STATE REQUEST primitive with "User-out-of-service" information.

If no "waiting for grant" is associated with the subsystem named in the *Subsystem-Out-of-Service-Grant* message, the *Subsystem-Out-of-Service-Grant* message is discarded and no further action is taken.

If the timer associated with the subsystem waiting for the grant expires before a *Subsystem-Out-of-Service-Grant* message is received, the "waiting for grant" is cancelled and the request is implicitly denied.

#### 5.3.5.3 *Actions at the requested node*

When the SCCP management at the node at which the backup subsystem is located receives the *Subsystem-Out-of-Service-Request* message, it checks the status of local resources[10]. If the SCCP has sufficient resources to assume the increased load, it invokes a N-COORD INDICATION primitive to the backup subsystem. If the SCCP does not have sufficient resources, no further action is taken[11].

---

[10] Local resources are whatever is critical to this particular node, and are implementation dependent.

[11] The possibility of introducing an explicit Subsystem-Out-of-Service-Denial message containing additional information and associated primitive is for further study.

If the backup system has sufficient resources to allow its mate to go out of service, it informs SCCP management by invoking a N-COORD RESPONSE primitive. A *Subsystem-Out-of-Service Grant* message is sent to SCCP management at the requesting node. If the backup subsystem does not have sufficient resources, no reply is returned [12].

### 5.3.6 *Local broadcast*

#### 5.3.6.1 *General*

The local broadcast procedure provides a mechanism to inform local allowed concerned subsystems of any related subsystem/signalling point status information received.

#### 5.3.6.2 *User-out-of-service*

A local broadcast of "User-out-of-service" information is initiated when:

a) a *Subsystem-Prohibited* message is received about a subsystem marked allowed (§ 5.3.2.2), or

b) an N-STATE REQUEST primitive with "User-out-of-service" information is invoked by a subsystem marked allowed (§ 5.3.2.2) [13], or

c) a local subsystem failure is detected by SCCP management (§ 5.3.2.2) [13],

d) an MTP-PAUSE indication primitive is received (§ 5.2.2).

SCCP management then informs local allowed concerned SCCP subsystems about the subsystem status by invoking N-STATE indication primitive with "User-out-of-service" information.

#### 5.3.6.3 *User-in-service*

A local broadcast of "subsystem-in-service" information is initiated when:

a) a *Subsystem-Allowed* message is received about a subsystem marked prohibited (§ 5.3.3), or

b) an N-STATE REQUEST primitive with "User-in-service" information is invoked by a subsystem marked prohibited (§ 5.3.3).

SCCP management then informs local allowed concerned SCCP subsystems, except the newly allowed one, about the subsystem status by invoking an N-STATE indication primitive with "User-in-service" information.

#### 5.3.6.4 *Signalling point inaccessible*

A local broadcast of "signalling point inaccessible" information is initiated when an MTP-RESUME primitive is received. SCCP management then informs local allowed concerned SCCP subsystems about the signalling point status by invoking an N-PCSTATE INDICATION primitive with "signalling point accessible" information.

#### 5.3.6.5 *Signalling point accessible*

A local broadcast of "signalling point accessible" information is initiated when an MTP-RESUME primitive is received. SCCP management then informs local allowed concerned SCCP subsystems about the signalling point status by invoking an N-PCSTATE INDICATION primitive with "signalling point accessible" information.

#### 5.3.6.6 *Signalling point congested*

A local broadcast of "signalling point congested" information is initiated when an MTP-STATUS primitive is received. SCCP management then informs local allowed concerned SCCP subsystems about the signalling point status by invoking an N-PCSTATE indication primitive with "signalling point congested (level)" information.

---

[12] The possibility of introducing an explicit Subsystem-Out-of-Service-Denial message containing additional information and associated primitive is for further study.

[13] These cases are applicable when the SCCP is used for routing between local subsystems. This function is implementation dependent.

5.3.7 *Broadcast*

5.3.7.1 *General*

The broadcast procedure provides a mechanism that may be used to inform concerned signalling points of any related subsystem status change at local or adjacent signalling points. It is an optional procedure supplementary to that defined in § 5.3.2.1. This procedure is suggested not to be used on a signalling point restart. This matter is for further study.

In some circumstances, the number of concerned signalling points is zero and no broadcast is performed. The action taken in this case is described in § 5.1.

5.3.7.2 *Subsystem prohibited*

A broadcast of *Subsystem-Prohibited* messages is initiated when:

a) a *Subsystem Prohibited* message is received about a subsystem presently marked allowed (§ 5.3.2.2), and the affected point code identified in the SSP message is the same as that of the informer signalling point, or

b) an N-STATE REQUEST primitive with "User-out-of-service" information is invoked by a subsystem marked allowed (§ 5.3.2.2), or

c) a local subsystem failure is detected by SCCP management § 5.3.2.2), or

d) a *Subsystem-Out-of-Service-Grant* message arrives for a subsystem marked "waiting for grant" (§ 5.3.5.2).

This broadcast permits SCCP management to inform all concerned signalling points, except the informer signalling point, about the subsystem status by *Subsystem-Prohibited* messages. SCCP management does not broadcast if the point code of the prohibited subsystem is different from that of the informer signalling point which originates the *Subsystem-Prohibited* message.

5.3.7.3 *Subsystem allowed*

A broadcast of *Subsystem-Allowed* messages is initiated when:

a) a *Subsystem-Allowed* message is received about a subsystem presently marked prohibited (§ 5.3.3), and the affected point code identified in the SSA message is the same as that of the informer signalling point, or

b) an N-STATE REQUEST primitive with "User-in-service" information is invoked by a subsystem marked prohibited (§ 5.3.3).

This broadcast permits SCCP management to inform all concerned signalling points, except the informer signalling point, about the subsystem status by *Subsystem-Allowed* messages. SCCP management does not broadcast if the point code of the allowed subsystem is different from that of the informer signalling point which originates the *Subsystem-Allowed* message.

5.4 *SCMG restart*

*Note* – This section is for further study.)

On a signalling point restart, an indication is given to the SCCP by the MTP about the signalling points which are accessible after the restart actions. For each accessible, concerned signalling point, all subsystems there are marked allowed. The response method is used to determine the status of SCCP subsystems in those signalling points in the absence of the receipt of subsystem allowed, and subsystem prohibited messages, which may have been broadcast from them.

At the restarted signalling point, the status of its own subsystems are not broadcast to concerned signalling points. In this case, the response method is used to inform other nodes attempting to access prohibited subsystems at the restarted signalling points.

The SCCP management procedures specified in Recommendation Q.714, § 5.2, describe the normal operation of management procedures, and do not describe signalling point restart actions.

ANNEX A

(to Recommendation Q.714)

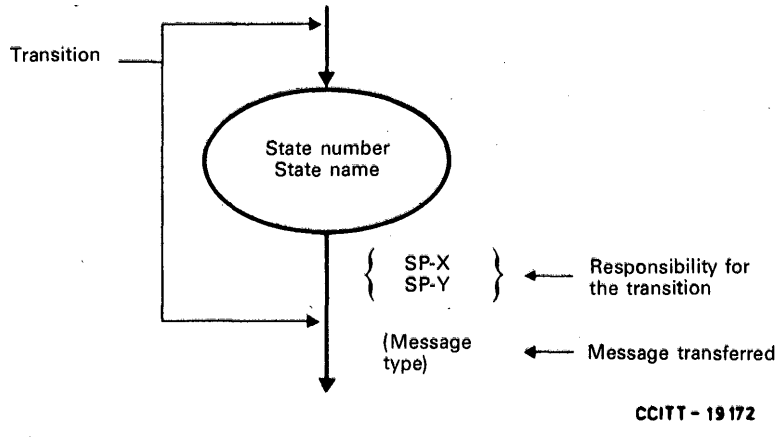
**State diagrams for the signalling connection control part of Signalling System No. 7**

A.1 *Introduction*

This Annex contains the definitions for the symbols used and defines the states of the signalling point X/Y interface and the transitions between states in the normal case.

Annex B contains the full definition of actions, if any, to be taken on the receipt of messages by a signalling point.

A.2 *Symbol definition of the state diagrams at the message interface between two nodes (signalling points: X and Y)* (see Figures A-1/Q.714 and A-2/Q.714)

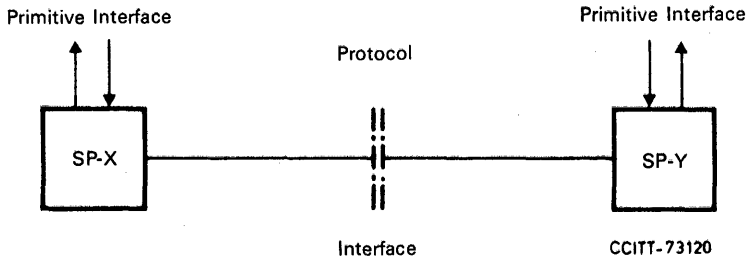



*Note 1* – Each state is represented by an ellipse wherein the state name and number are indicated.

*Note 2* – Each state transition is represented by an arrow. The responsibility for the transition (SP-X or SP-Y) and the message that has been transferred is indicated beside that arrow.

FIGURE A-1/Q.714

**Symbol definition of the state diagram**




*Note* — SP-X and SP-Y are the signalling points X and Y denoting respectively the origin and destination of the connection section concerned.

FIGURE A-2/Q.714

**Primitive and protocol interfaces**

A.3 *Order definition of the state diagrams*

For the sake of clarity, the normal procedure at the interface is described in a number of small state diagrams. In order to describe the normal procedure fully, it is necessary to allocate a priority to the different figures and to relate a higher order diagram with a lower one. This has been done by the following means:

- Figures A-3/Q.714, A-4/Q.714, A-5/Q.714 and A-6/Q.714 are arranged in order of priority, with Figure A-3/Q.714 having the highest priority and subsequent figures having lower priority. Priority means that when a message belonging to a higher order diagram is transferred, that diagram is applicable and the lower order one is not.
- The relation with a state in a lower order diagram is given by including that state inside an ellipse in the higher order diagram.
- The message abbreviations are those defined in Recommendation Q.712.

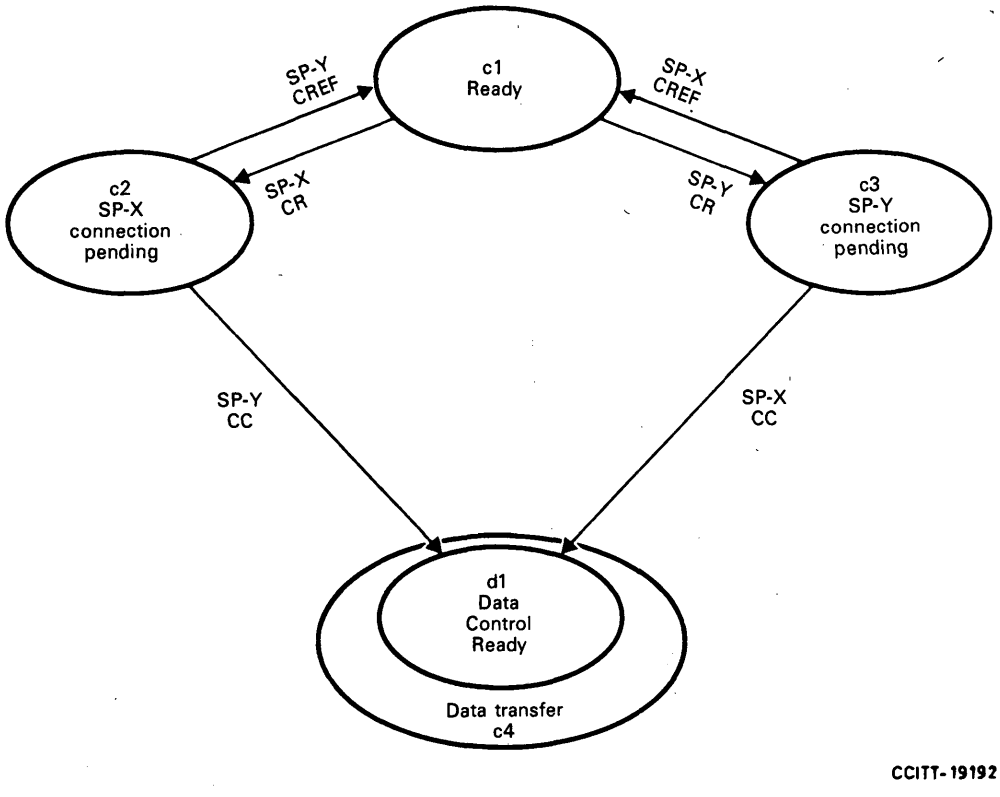
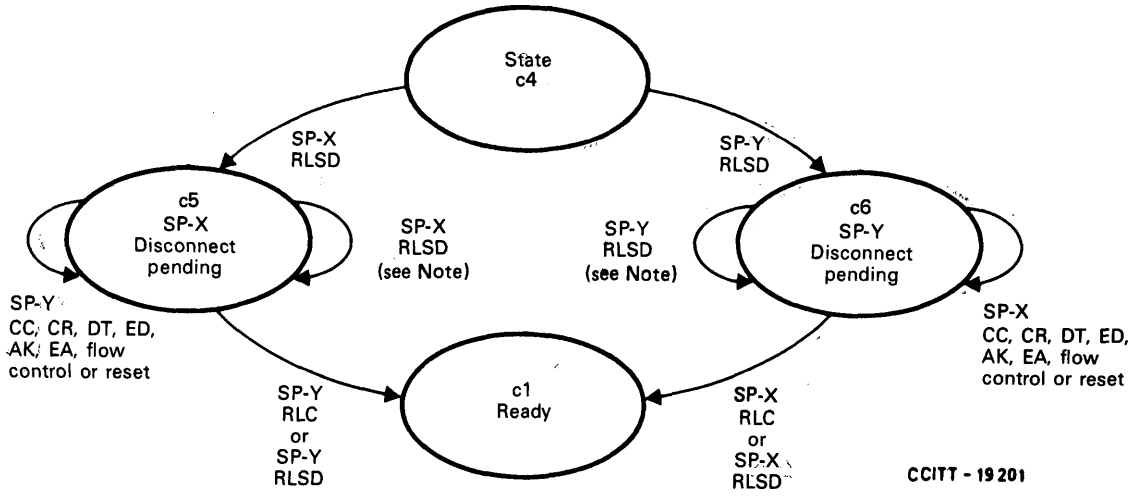



FIGURE A-3/Q.714

**State transition diagram for sequences of messages during connection establishment**




*Note* — This transition may take place after time-out.

FIGURE A-4/Q.714

**State transition diagram for sequences of messages during connection release**

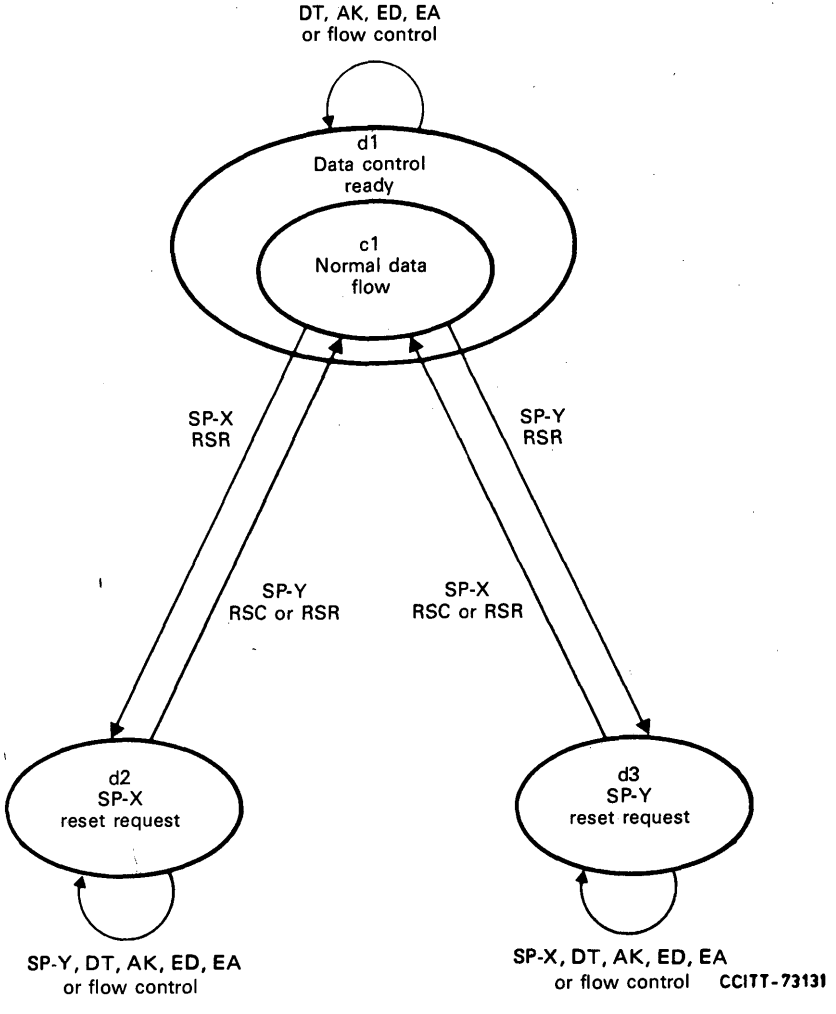



FIGURE A-5/Q.714

**State transition diagram for the transfer of reset messages within the data transfer (c4) state**

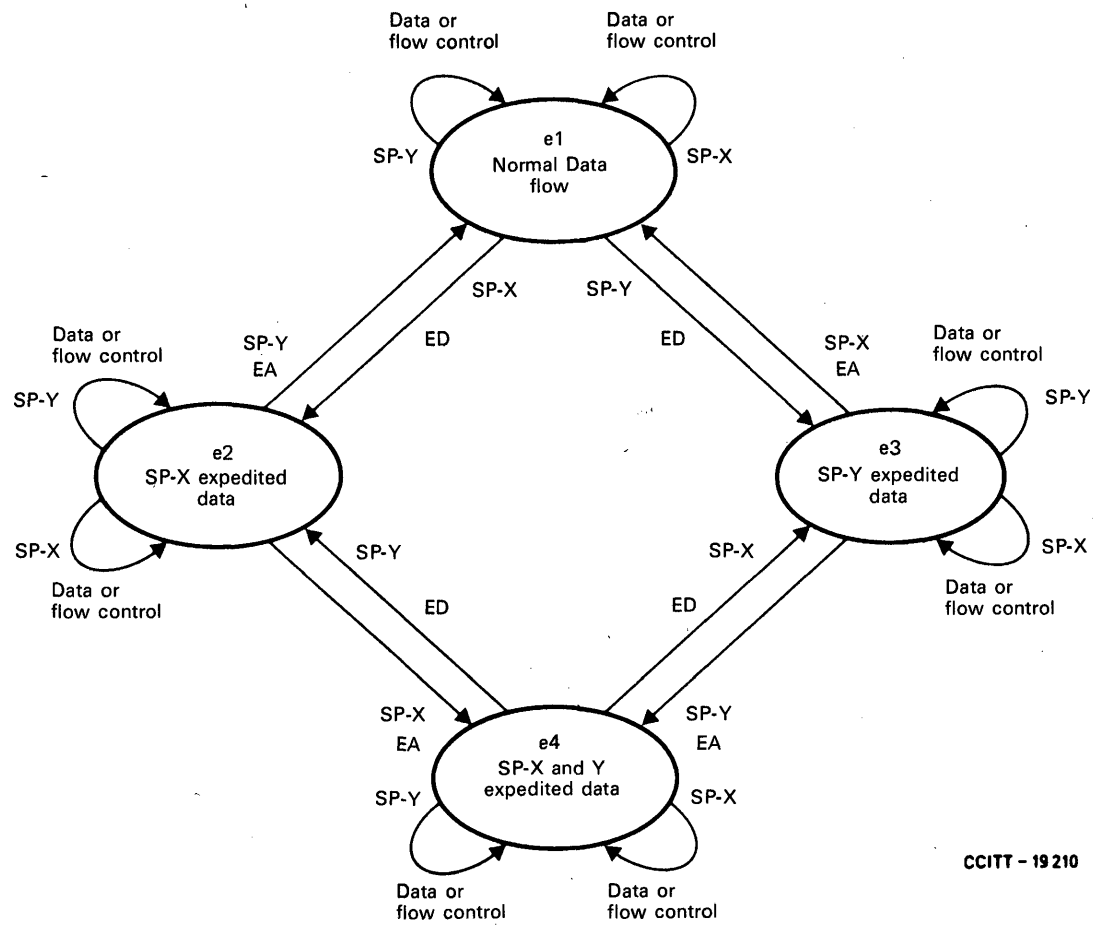



FIGURE A-6/Q.714

**State transition diagram for the transfer of data, expedited data and flow control within the data transfer (c4) state**

ANNEX B

(to Recommendation Q.714)

## Action tables for the signalling connection control part of Signalling System No. 7

### B.1 *Introduction*

This Annex contains the definitions for the symbols used and contains the full definition of actions, if any, to be taken on the receipt of messages by a signalling point (node).

Annex A contains the full definition of states of the signalling point X/Y interface and the transitions between states in the normal case.

### B.2 *Symbol definition of the action tables*

The entries given in Table B-1/Q.714 and B-2/Q.714 indicate the action, if any, to be taken by a SP on receipt of any kind of message, and the state the SP enters, which is given in parentheses, following the action taken.

In any state it is possible to receive an Error message (ERR). The reaction, if any, depends on the contents (error cause and possible diagnostics) of the message and is specified in Q.714, § 3.10.3.

The reaction on messages received with procedure errors (e.g. too long, invalid P(R), not octet aligned, etc.) are normal actions and will be described in the text. So they are covered by the actions indicated as NORMAL.

B.3 *Table of contents*



TABLE B-1/Q.714

**Action taken by SP-Y on receipt of messages**

| State of the interface as perceived by node SP-Y / Message received by node SP-Y | Any state |
|---|---|
| Any message with unknown message type (see Note) | DISCARD |
| Any message with known message type and:<br>a) unassigned destination local reference number, or<br>b) Originating Point Code received not equal to the PC stored locally, or<br>c) source local reference number received not equal to the remote local reference number stored locally | See Table B-2/Q.714 |
| Any other message | See Table B-3/Q.714 |

DISCARD: SP-Y discards the received message and takes no subsequent action.

*Note* – This notion of unknown message type depends upon the protocol class.

TABLE B-2/Q.714

**Action taken by SP-Y on receipt of messages with known message type and containing mismatch information as in Table B-1/Q.714 in any state**

| Type of mismatch information / Message received by node PS-Y | Unassigned destination local reference number | Source local reference number received not equal to the one stored locally | Originating Point Code received not equal to the PC stored locally (see Note 1) |
|---|---|---|---|
| CR (X) | N.A. | N.A. | N.A. |
| CC (Y, X) | Send ERR (X) (see Note 2) | N.A. | N.A. |
| CREF (Y) | DISCARD | N.A. | N.A. |
| RLSD (Y, X) | Send RLC (X, Y) (see Note 2) | Send ERR (X) (see Note 2) | Send ERR (X) (see Note 2) |
| RLC (Y, X) | DISCARD | DISCARD | DISCARD |
| DT1 (Y) | DISCARD | N.A. | C.O.N.P. |
| DT2 (Y) | DISCARD | N.A. | C.O.N.P. |
| AK (Y) | DISCARD | N.A. | C.O.N.P. |
| ED (Y) | DISCARD | N.A. | C.O.N.P. |
| EA (Y) | DISCARD | N.A. | C.O.N.P. |
| RSR (Y, X) | Send ERR (X) (see Note 2) | Send ERR (X) (see Note 2) | Send ERR (X) (see Note 2) |
| RSC (Y, X) | Send ERR (X) (see Note 2) | Send ERR (X) (see Note 2) | Send ERR (X) (see Note 2) |
| ERR (Y) | For further study | For further study | For further study |
| IT (Y, X) | DISCARD | RELEASE | C.O.N.P |

DISCARD: SP-Y discards the received message and takes no subsequent action.

C.O.N.P. Check Optionally Not Performed.

N.A. Not Applicable

NAME (d, s): NAME = abbreviation of message
d = destination local reference number
s = source local reference number.

*Note 1* – Performing this check is a national option.

*Note 2* – In this situation no action is taken locally on any existing connection section. Information in any message sent back is taken from the received message.

TABLE B-3/Q.714

**Action taken by SP-Y on receipt of messages during connection establishment and release phases**

| State of the interface as perceived by node SP-Y / Message received by note SP-Y | Signalling connection control ready: r1 | | | | | |
|---|---|---|---|---|---|---|
| | Ready c1 | SP-X connection pending c2 | SP-Y connection pending c3 | Data transfer c4 | SP-X disconnect pending c5 | SP-Y disconnect pending c6 |
| Connexion request (CR) | NORMAL (c2) | See Note | | | | |
| Connection confirm (CC) | See Table B-2/Q.714 | DISCARD (c2) | NORMAL (c4) | DISCARD (c4) | ERROR 1 (c6) | DISCARD (c6) |
| Connection refused (CREF) | | DISCARD (c2) | NORMAL (c1) | DISCARD (c4) | ERROR 1 (c6) | DISCARD (c6) |
| Released (RLSD) | | DISCARD (c2) | ERROR 2 (c3) | NORMAL (c5) | DISCARD (c5) | NORMAL (c1) |
| Released complete (RLC) | | DISCARD (c2) | ERROR 3 (c1) | DISCARD (c4) | ERROR 1 (c6) | NORMAL (c1) |
| Other messages | | DISCARD (c2) | ERROR 3 (c1) | See Table B-4/Q.714 | ERROR 1 (c6) | DISCARD (c6) |

NORMAL: The action taken by SP-Y follows the normal procedures as defined in the appropriate sections of the procedure text.

DISCARD: SP-Y discards the received message and takes no subsequent action.

ERROR 1: SP-Y discards the received message and initiates a connection release by sending a RLSD message with proper invalid type cause.

ERROR 2: SP-Y returns a Released complete message using information contained in the message and takes no subsequent action.

ERROR 3: SP-Y discards the received message and releases locally.

*Note* – Reception of CR in these states is note possible because CR does not contain a destination local reference number (no search is performed).

TABLE B-4/Q.714

**Action taken by node SP-Y as receipt of messages during the data transfer state**

| State of the interface as perceived by node SP-Y / Message received by node SP-Y | Data transfer: c4 | | |
|---|---|---|---|
| | Data control ready (d1) | SP-X reset request (d2) | SP-Y reset request (d3) |
| Reset request (RSR) (see Note 2) | NORMAL (d2) | DISCARD (d2) | NORMAL (d1) |
| Reset confirmation (RSC) (see Note 2) | ERROR (d3) | ERROR (d3) | NORMAL (d1) |
| Other messages | See Table B-5/Q.714 | ERROR (d3) (see Note 1) | DISCARD (d3) |

NORMAL: The action taken by SP-Y follows the normal procedures as defined in the appropriate sections of the procedure text.

DISCARD: Signalling point Y discards the received message and takes no subsequent action.

ERROR: Signalling point Y discards the received message and initiates a reset by transmitting a reset request message with the appropriate cause indication.

*Note 1* – If signalling point Y issues a reset by transmitting a reset request message as a result of an error condition in state d2, it should eventually consider the interface to be in the Data control ready state (d1).

*Note 2* – Reception of these messages for a class 2 connection section may trigger the sending of an ERR message back if these message types are known by the receiving SCCP.

TABLE B-5/Q.714

**Action taken by SP-Y on receipt of messages during the data control ready state**

| State of the interface as perceived by node SP-Y / Message received by node SP-Y | Data control ready: d1 | | | |
|---|---|---|---|---|
| | Normal data flow e1 | SP-X expedited data e2 | SP-Y expedited data e3 | SP-X and SP-Y expedited data e4 |
| Expedited data (ED) | NORMAL (d2) | ERROR (d3) | NORMAL (d4) | ERROR (d3) |
| Expedited data (EA) acknowledgement | DISCARD (e1) | DISCARD (e2) | NORMAL (e1) | NORMAL (e2) |
| Data (DT), data acknowledgement (AK) and Inactivity Test (IT) | NORMAL (e1) | NORMAL (e2) | NORMAL (e3) | NORMAL (e4) |

NORMAL: The action taken by signalling point Y follows the normal procedures as defined in the appropriate sections of the procedure text.

DISCARD: Signalling point Y discards the received message and takes no subsequent action as direct result of receiving that message.

ERROR: Signalling point Y discards the received message packet and indicates a reset by transmitting a reset request message with the appropriate cause indication (e.g. procedure error).

*Note* – Reception of an ED, EA, $DT_2$ or AK message for a class 2 connection section will cause the receiving SCCP to DISCARD any of these messages. A $DT_1$ message received for a class 3 connection section will also be discarded.

ANNEX C

(to Recommendation Q.714)

**State transition diagrams (STD)
for the signalling connection control part of
Signalling System No. 7**

C.1 *General*

This annex contains the description of the main SCCP functions (except SCCP management (SCMG) which is contained in annex D to Recommendation Q.714) according to the CCITT Specification and Description Language (SDL).

For the SCCP as a whole, Figure 1/Q.714 illustrates a subdivision into functional blocks, showing their functional interactions as well as the functional interactions with the other major functions of signalling system No. 7 (e.g. MTP).

The functional breakdown shown in this diagram is intended to illustrate a reference model, and to assist interpretation of the text of the SCCP procedures. The state transition diagrams are intended to show precisely the behaviour of the signalling system under normal and abnormal conditions as viewed from a remote location. It must be emphasized that the functional partitioning shown in the following diagrams is used only to facilitate understanding of the system behaviour, and is not intended to specify the functional partitioning to be adopted in a practical implementation of the signalling system.

C.2 *Drafting conventions*

Each major function is designated by its acronym (e.g. SCOC = SCCP connection-oriented control).

External inputs and outputs are used for interactions between different functional blocks. Included within each input and output symbol in the state transition diagrams are acronyms which identify the functional blocks which are the source and the destination of the message, e.g.:

SCRC → SCOC indicates that the message is sent from SCCP routing control to SSCP connection-oriented control

Internal inputs and outputs are only used to indicate control of timers.

C.3 *Figures*

The list of figures is as follows:

Figure C-1/Q.714 SCCP routing control procedures (SCRC).

Figure C-2/Q.714 Connection establishment and release procedures at originating node for SCCP connection-oriented control (SCOC).
(Sheets 1 to 3: connection establishment, and sheets 4 to 6: connection release procedures)

Figure C-3/Q.714 Connection establishment and release procedures at destination node for SCCP connection-oriented control (SCOC).
(Sheets 1 to 2: connection establishment, and sheets 3 to 5: connection release procedures)

Figure C-4/Q.714 Data transfer procedures at originating and destination nodes for SCCP connection-oriented control (SCOC).

Figure C-5/Q.714 Expedited data transfer procedures at originating and destination nodes for SCCP connection-oriented control (SCOC).

Figure C-6/Q.714 Reset procedures at originating and destination nodes for SCCP connection-oriented control (SCOC).

Figure C-7/Q.714 Connection establishment and release procedures at intermediate node for SCCP connection-oriented control (SCOC).
(Sheets 1 to 4: connection establishment, and sheets 5 to 9: connection release procedures)

Figure C-8/Q.714 Data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC).

Figure C-9/Q.714 Expedited data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC).

Figure C-10/Q.714 Reset procedures at intermediate node for SCCP connection-oriented control (SCOC).

Figure C-11/Q.714 Restart procedure for SCCP connection-oriented control (SCOC).

Figure C-12/Q.714 SCCP connectionless control (SCLC).

## C.4 *Abbreviations and timers*

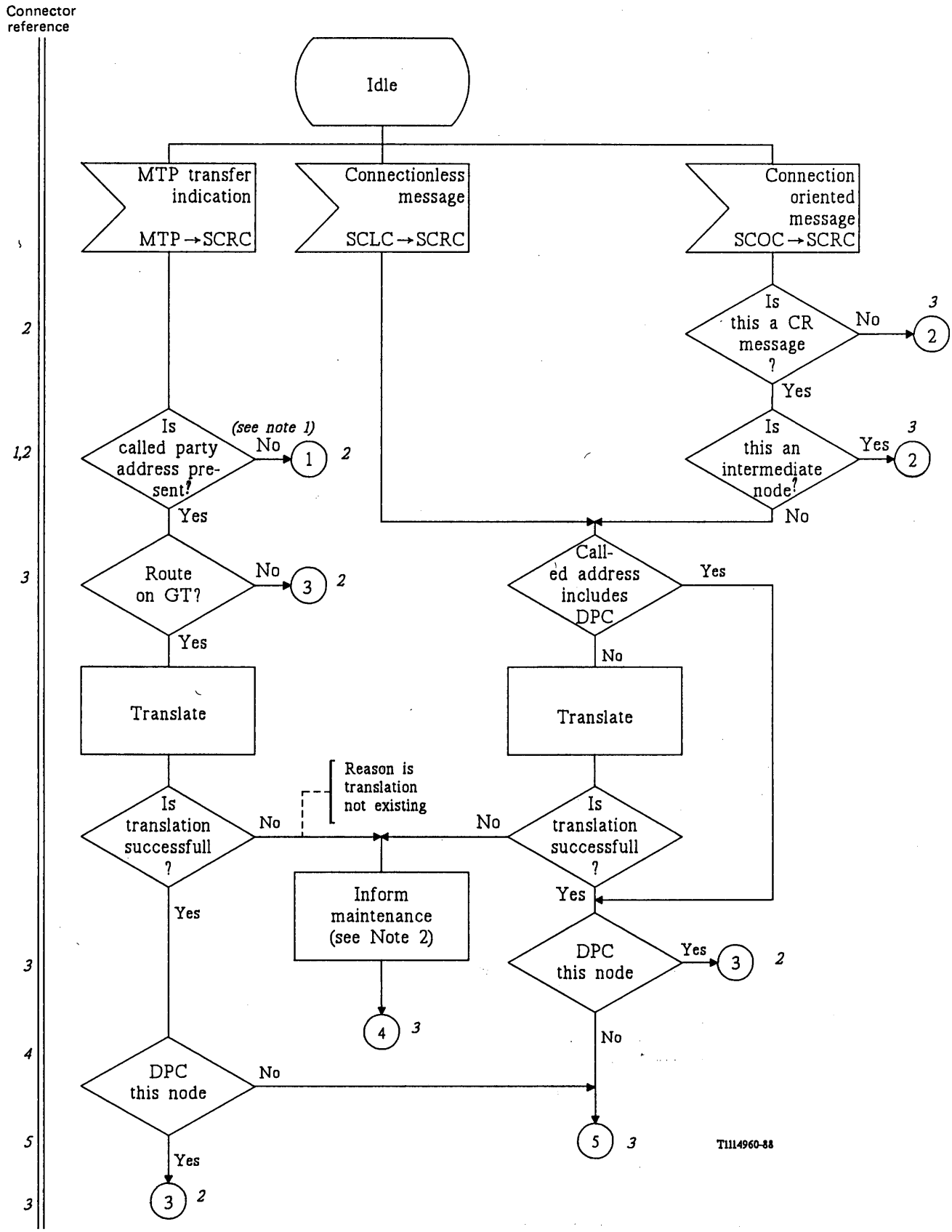
Abbreviations and timers used in Figures C-1/Q.714 to C-11/Q.714 are listed below.

*Abbreviations*

| | |
|---|---|
| CR | Connection Request |
| DPC | Destination Point Code |
| GT | Global Title |
| IT | Inactivity Test |
| MSG | Message |
| MTP | Message Transfer Part |
| NPDU | Network Protocol Data Unit |
| NSDU | Network Service Data Unit |
| PC | Point Code |
| SCCP | Signalling Connection Control Part |
| SCLC | SCCP Connectionless Control |
| SCMG | SCCP Management |
| SCOC | SCCP Connection-Oriented Control |
| SCRC | SCCP Routing Control |
| SLS | Signalling Link Selection |
| SS | Sub-System |
| SSN | Sub-System Number |
| SSPC | Sub-System Prohibited Control |

*Timers*

| | |
|---|---|
| T(conn est) | Waiting for connection confirm message. |
| T(ias) | Delay to send a message on a connection section. |
| T(iar) | Waiting to receive a message on a connection section. |
| T(rel) | Waiting for release complete message. |
| T(int) | Waiting to report abnormal release to maintenance function. |
| T(guard) | Waiting to resume normal procedures for temporary connection sections during the restart procedure |




*Note 1* – This will always be a connection oriented message excluding a CR message.

*Note 2* – Maintenance functions are for further study.

FIGURE C-1/Q.714 (Sheet 1 of 3)

**SCCP routing control procedures (SCRC)**

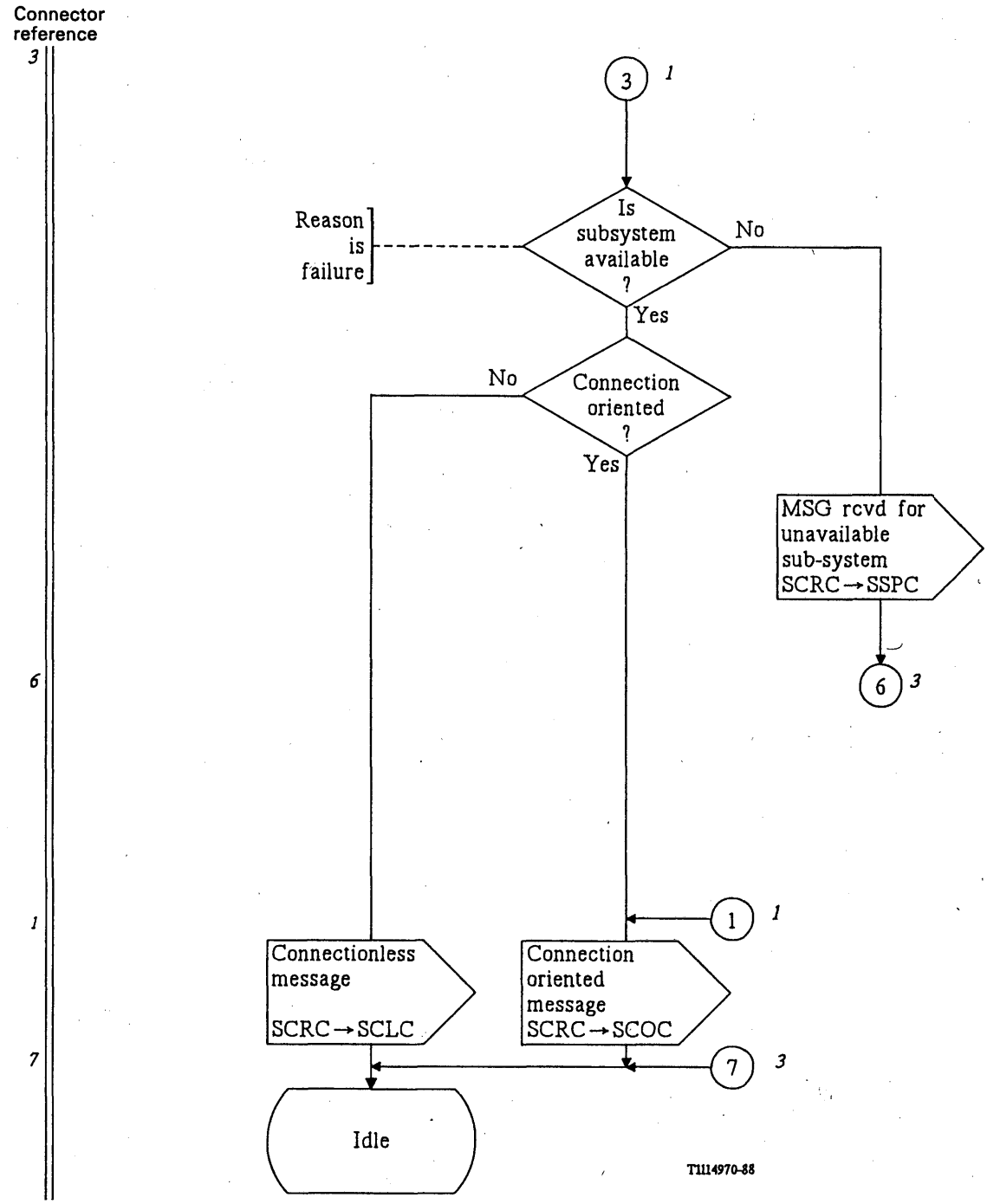
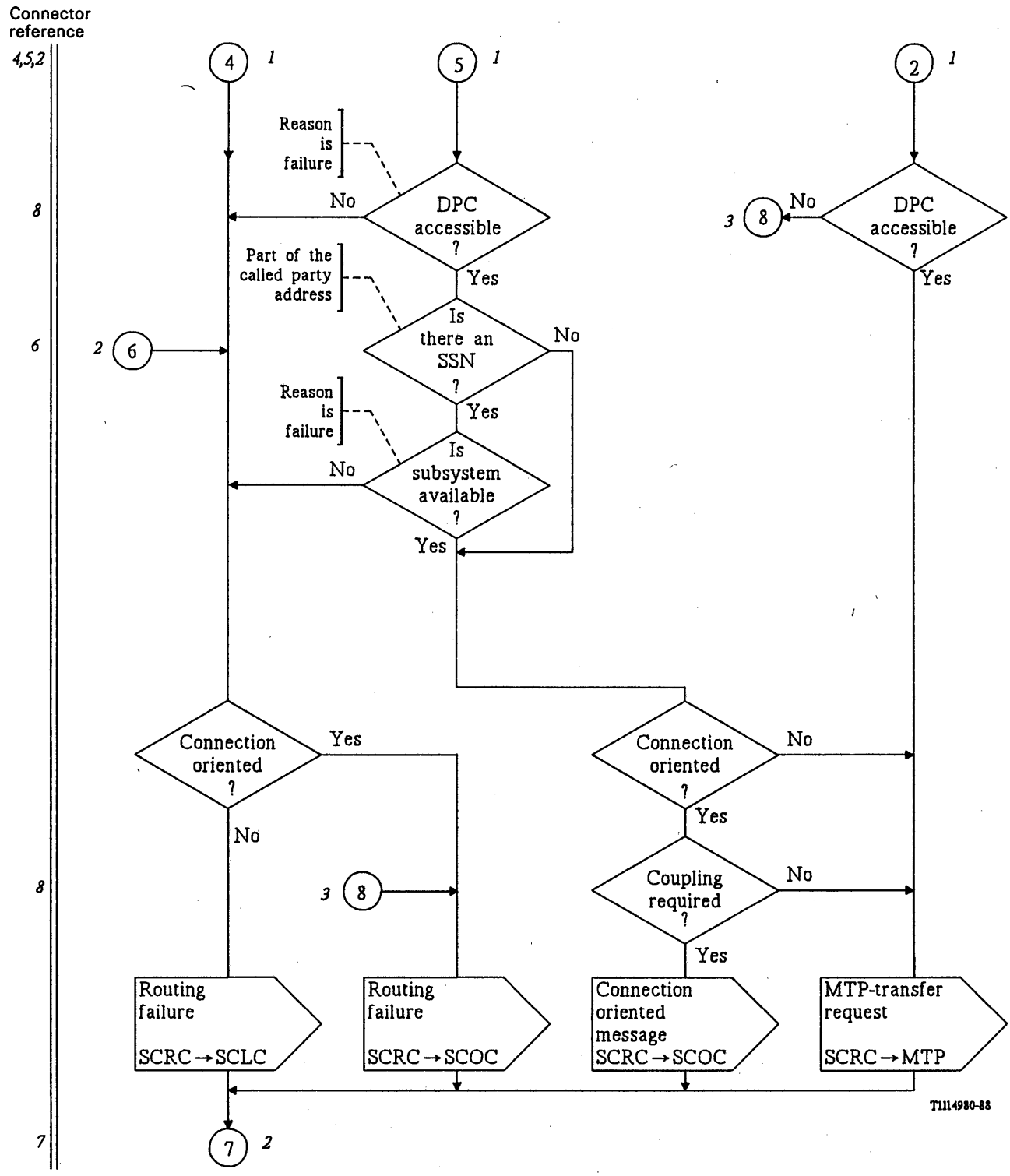



FIGURE C-1/Q.714 (Sheet 2 of 3)

**SCCP routing control procedures (SCRC)**




*Note* – Actions for a DPC congested are for further study.

FIGURE C-1/Q.714 (Sheet 3 of 3)

**SCCP routing control procedures (SCRC)**

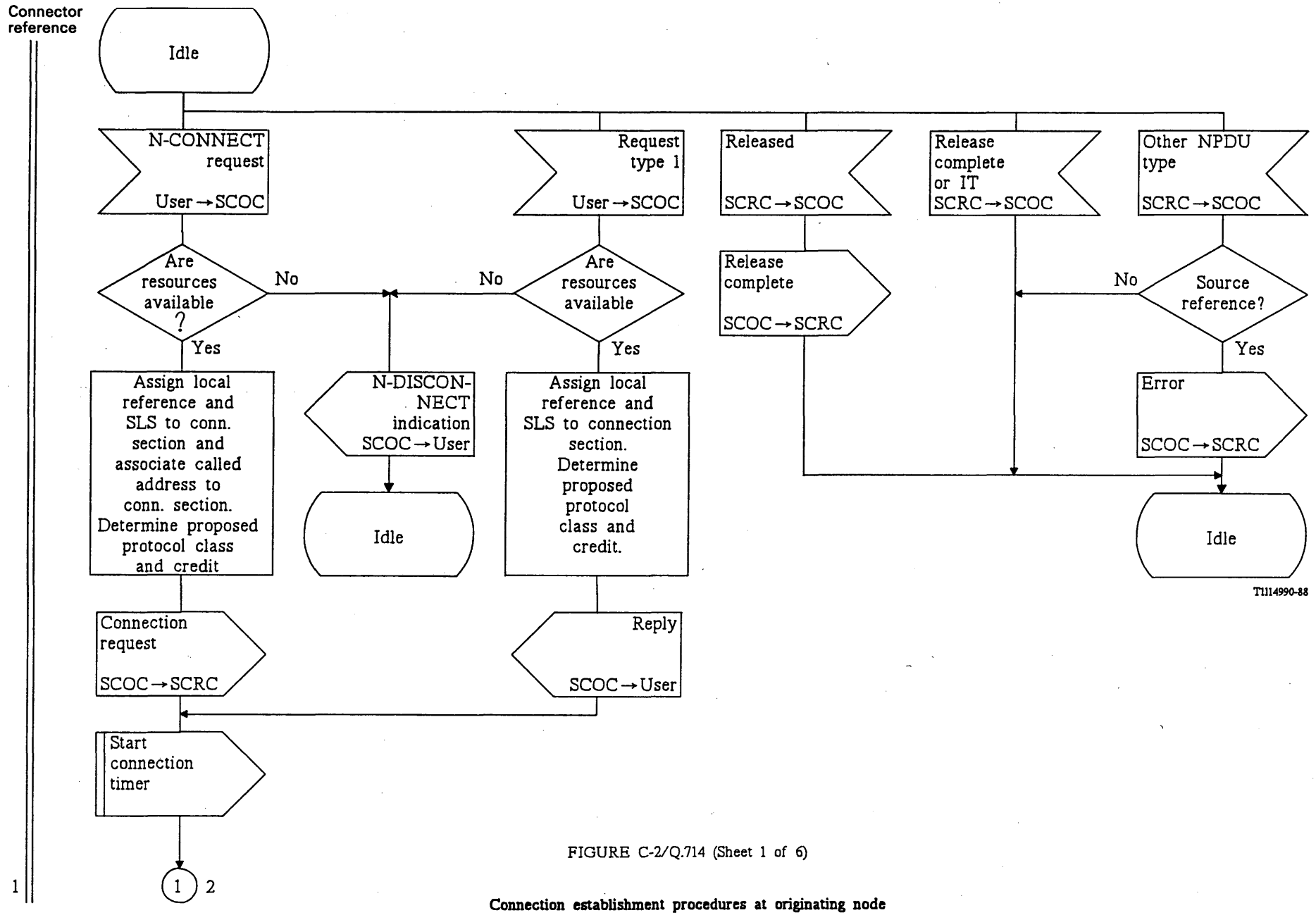
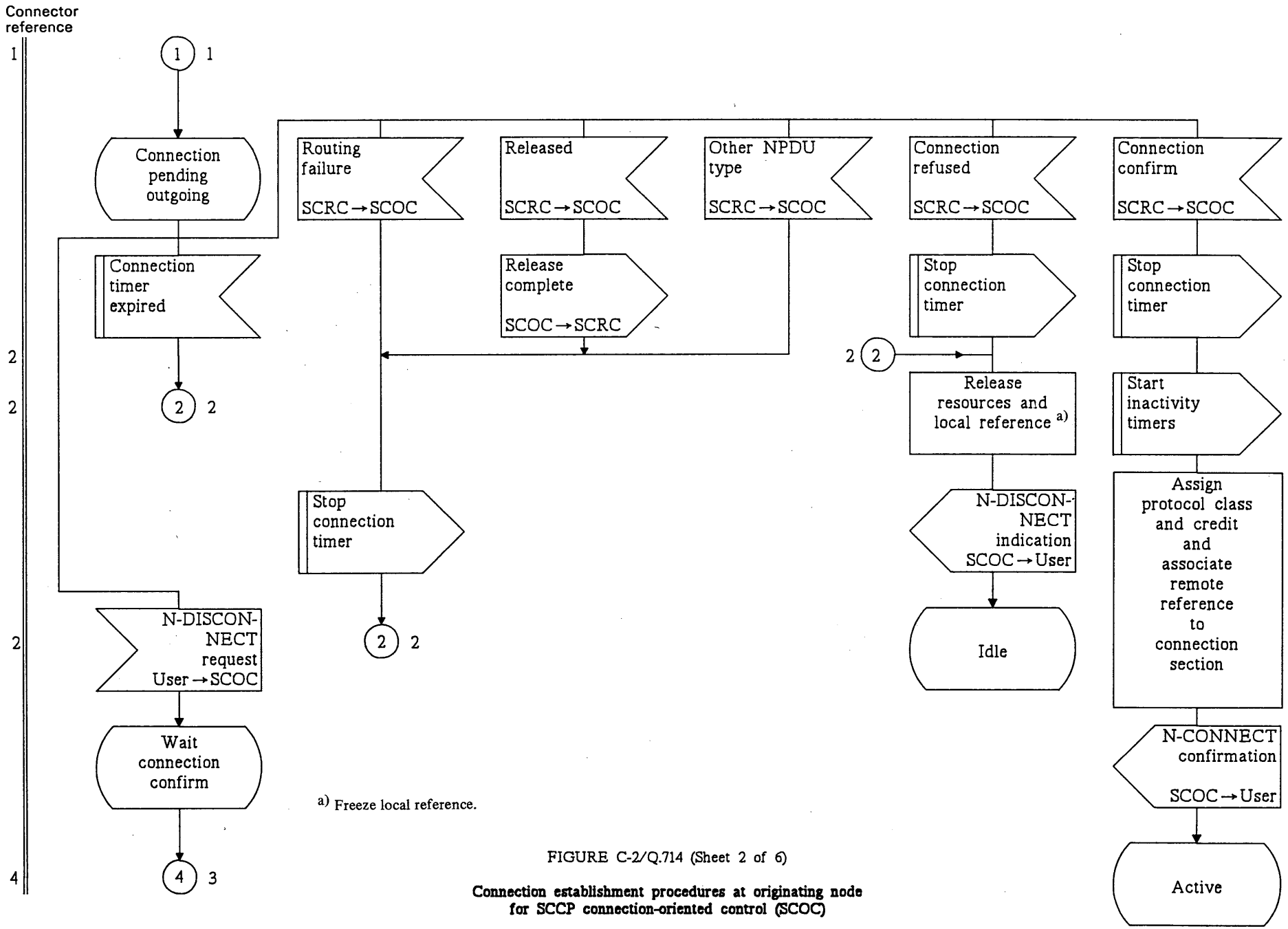



FIGURE C-2/Q.714 (Sheet 1 of 6)

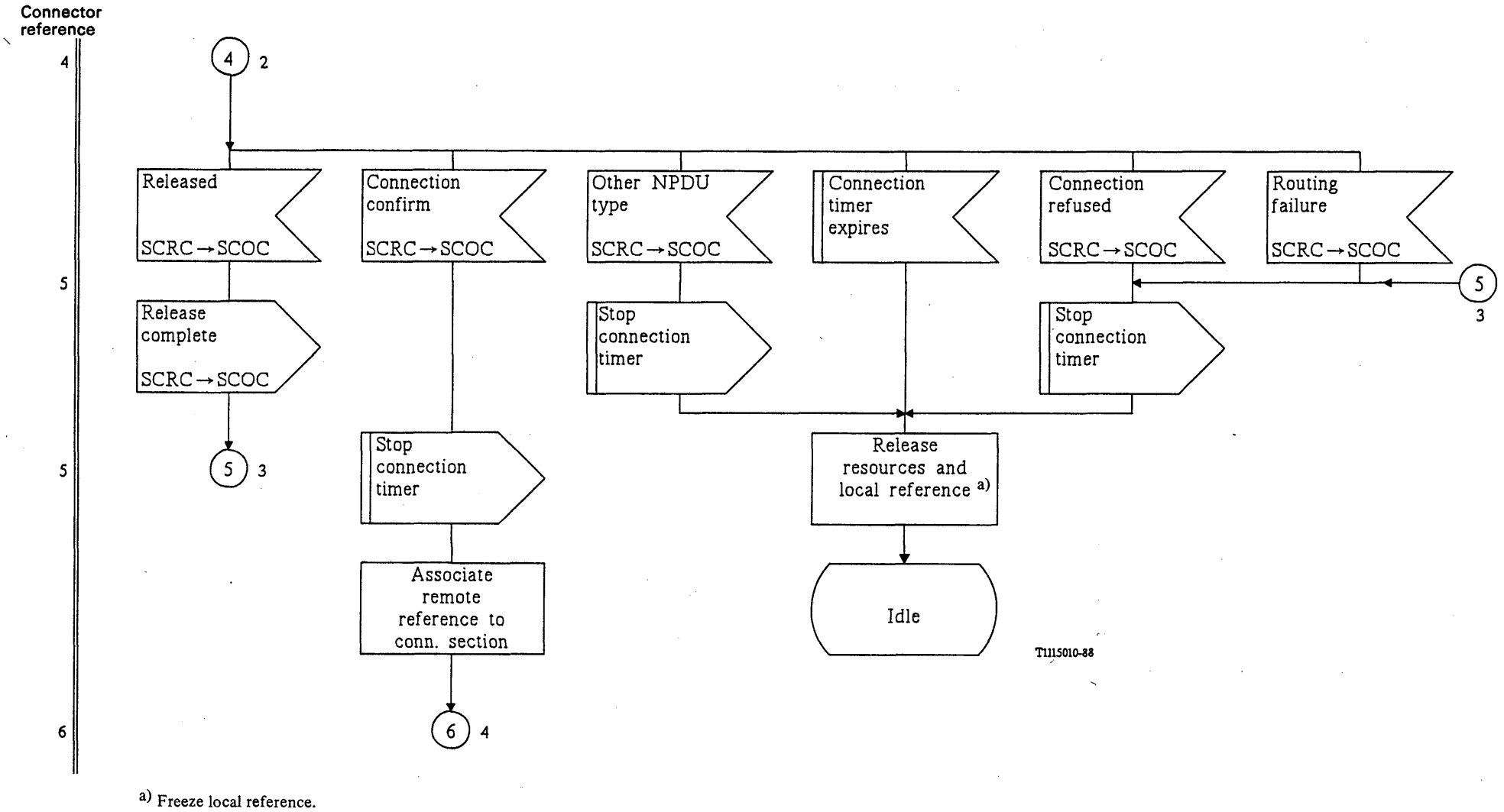
**Connection establishment procedures at originating node for SCCP connection-oriented control (SCOC)**




a) Freeze local reference.

FIGURE C-2/Q.714 (Sheet 2 of 6)

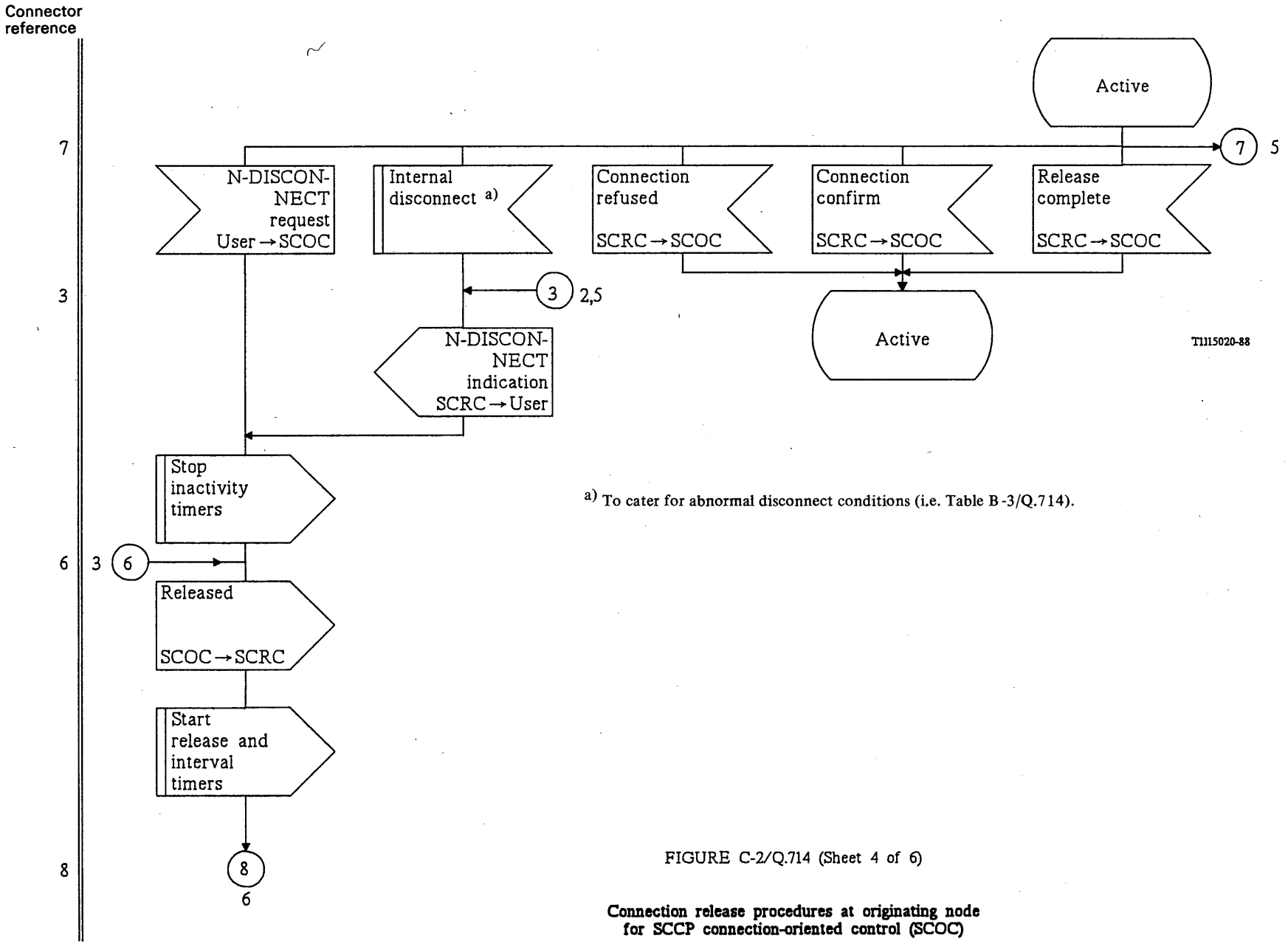
**Connection establishment procedures at originating node for SCCP connection-oriented control (SCOC)**




a) Freeze local reference.

FIGURE C-2/Q.714 (Sheet 3 of 6)

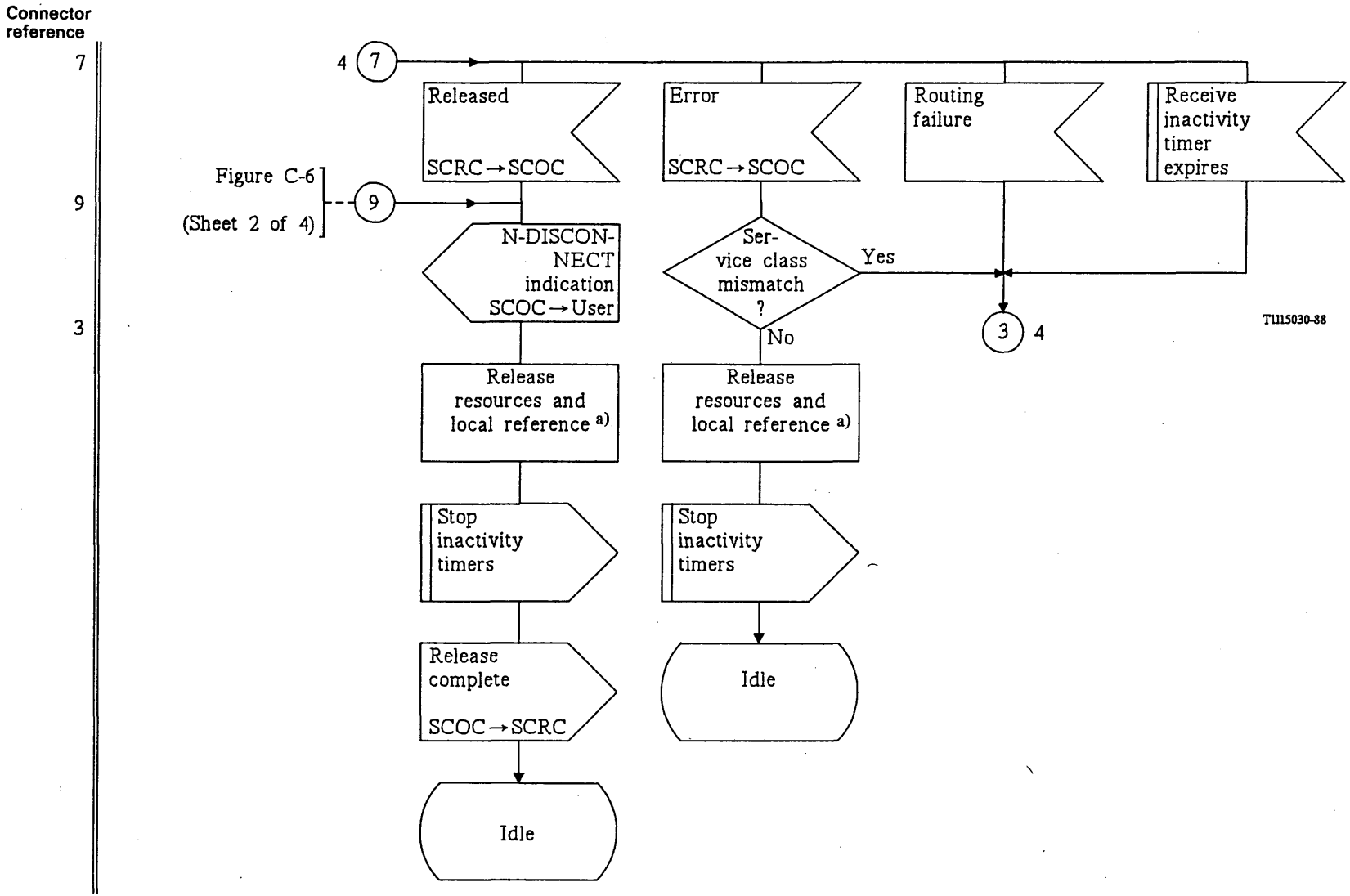
**Connection establishment procedures at originating node for SCCP connection-oriented control (SCOC)**




a) To cater for abnormal disconnect conditions (i.e. Table B-3/Q.714).

FIGURE C-2/Q.714 (Sheet 4 of 6)

**Connection release procedures at originating node for SCCP connection-oriented control (SCOC)**




a) Freeze local reference.

FIGURE C-2/Q.714 (Sheet 5 of 6)

**Connection release procedures at originating node for SCCP connection-oriented control (SCOC)**

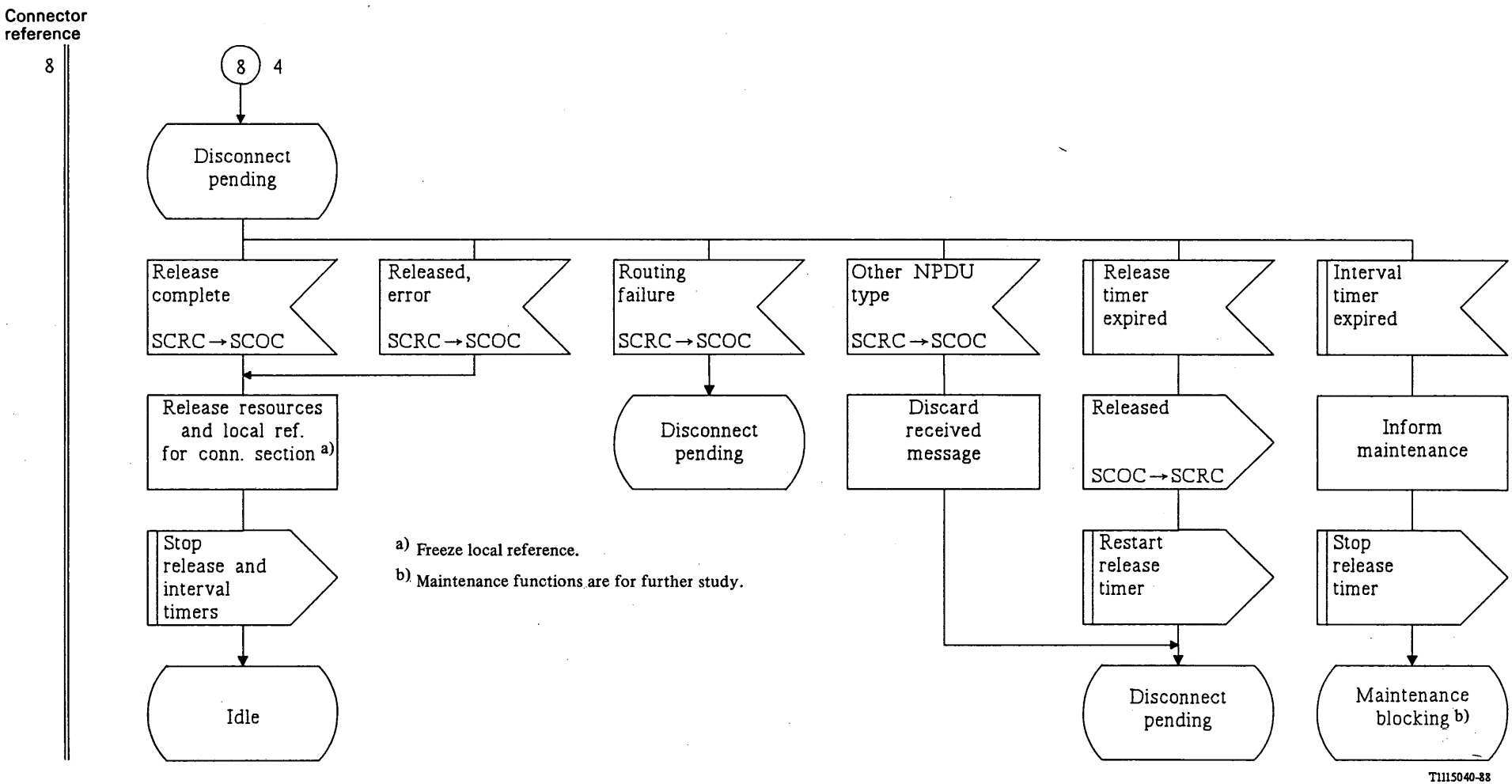
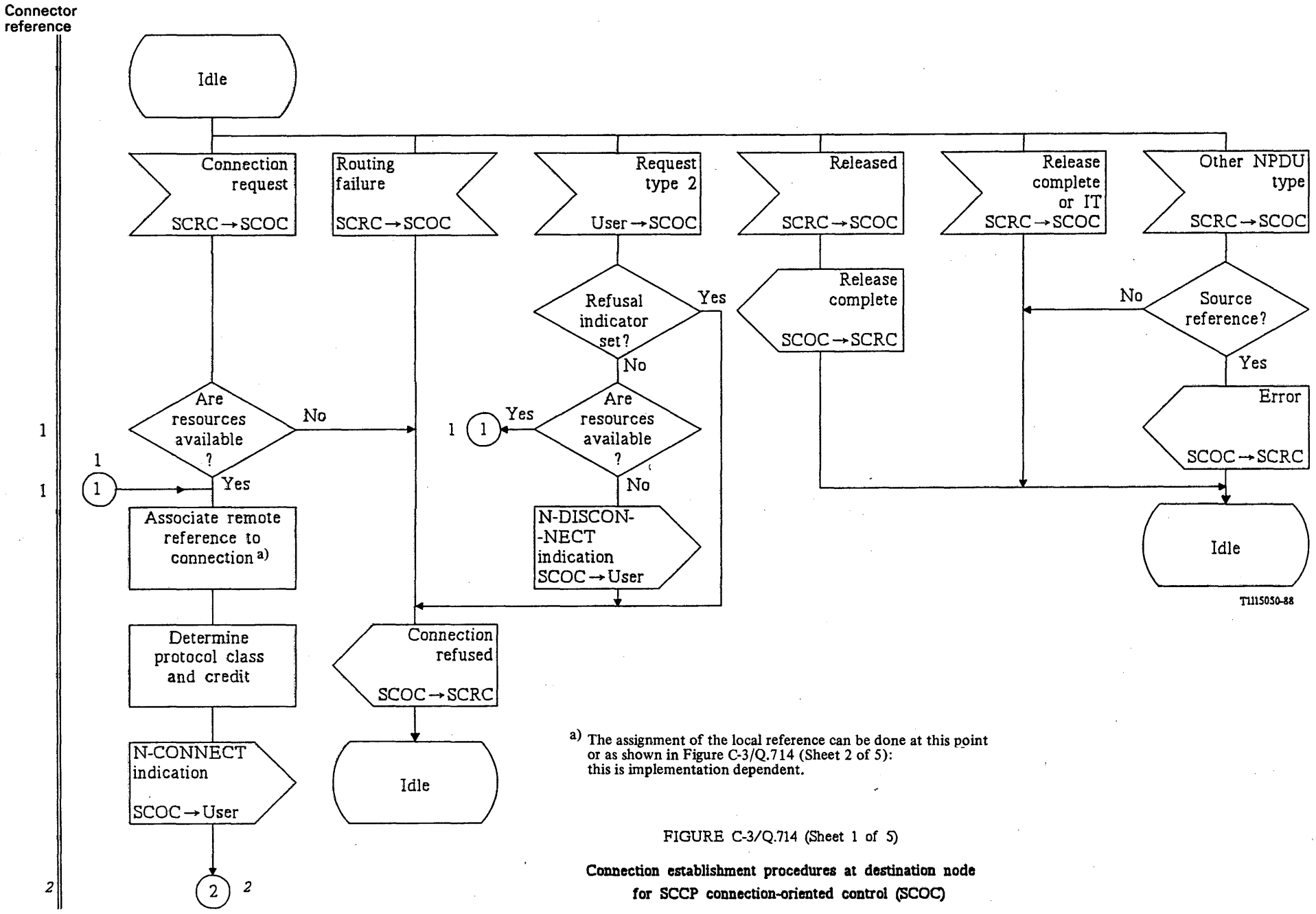



FIGURE C-2/Q.714 (Sheet 6 of 6)

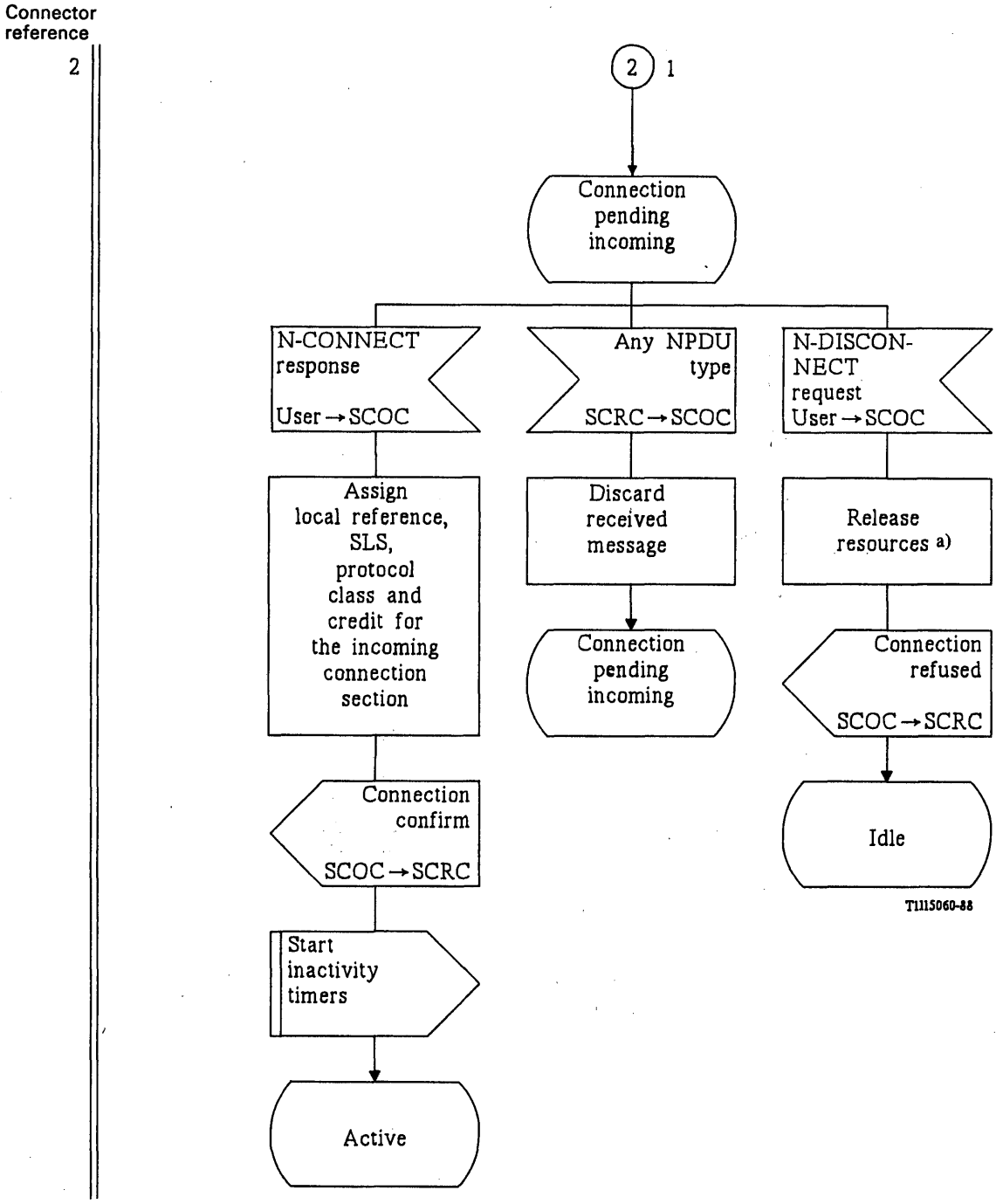
**Connection release procedures at originating node for SCCP connection-oriented control (SCOC)**




a) The assignment of the local reference can be done at this point or as shown in Figure C-3/Q.714 (Sheet 2 of 5): this is implementation dependent.

FIGURE C-3/Q.714 (Sheet 1 of 5)

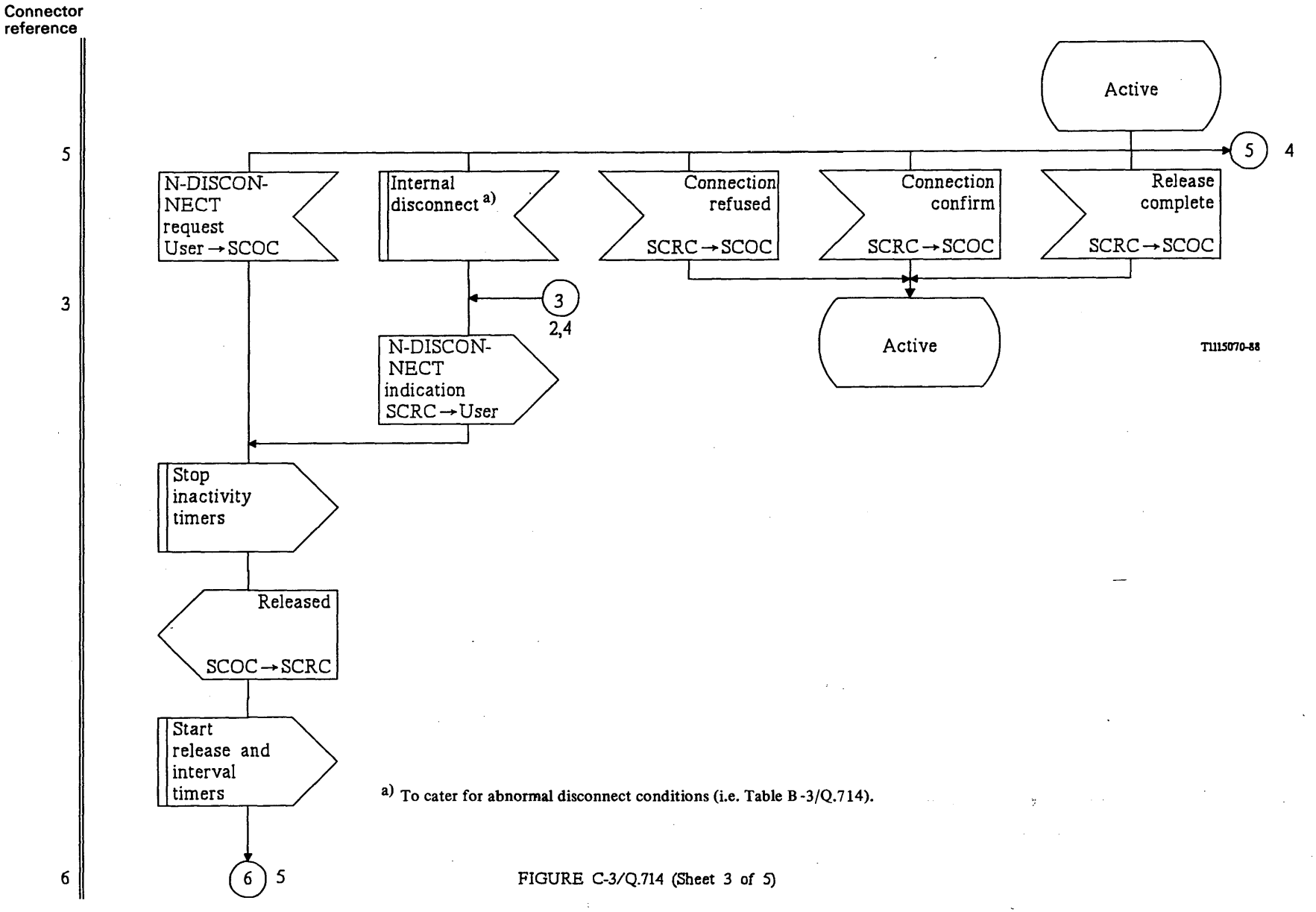
**Connection establishment procedures at destination node for SCCP connection-oriented control (SCOC)**




a) The local reference may have to be released and frozen if it has been previously assigned.

FIGURE C-3/Q.714 (Sheet 2 of 5)

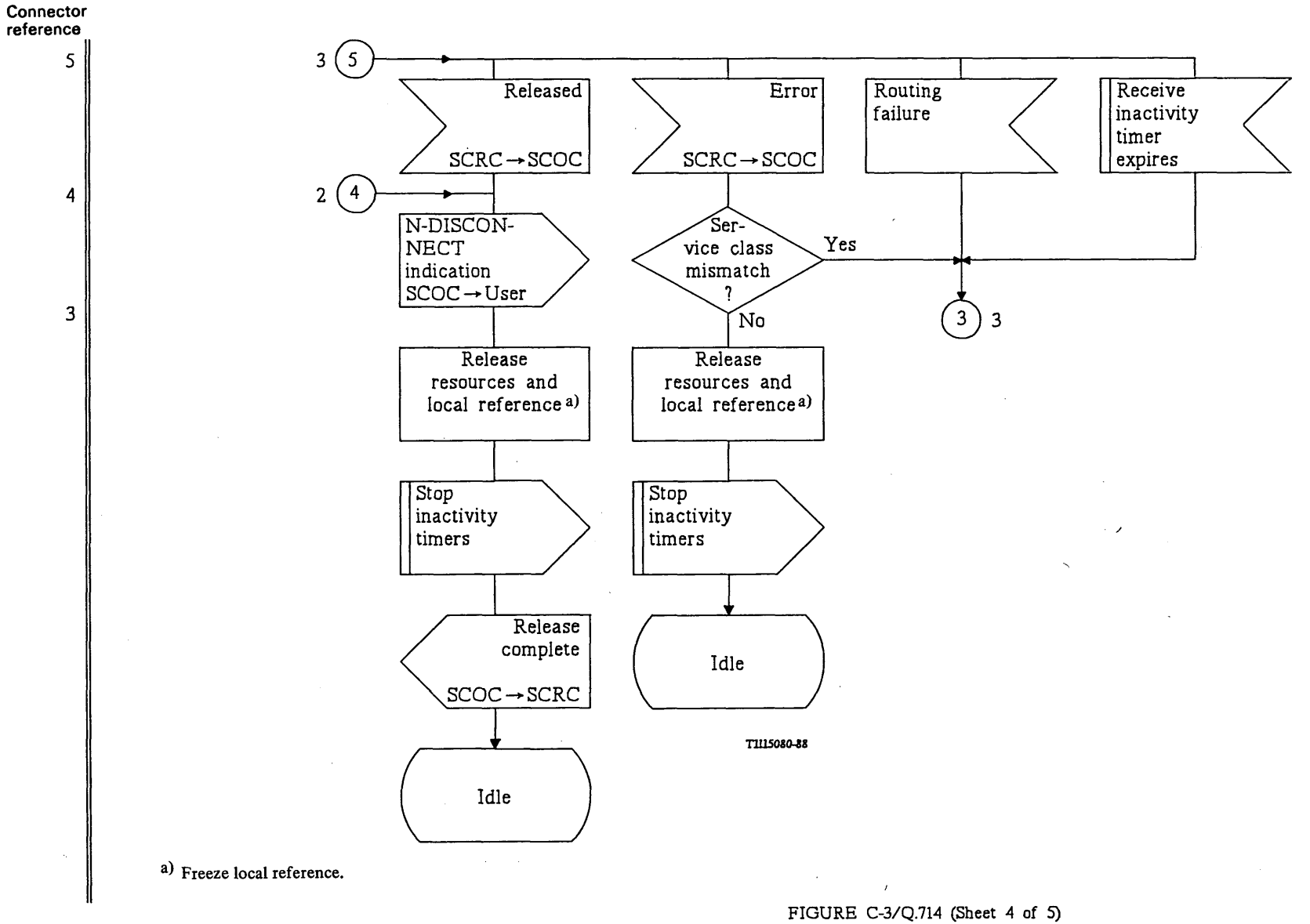
**Connection establishment procedures at destination node for SCCP connection-oriented control (SCOC)**




a) To cater for abnormal disconnect conditions (i.e. Table B-3/Q.714).

FIGURE C-3/Q.714 (Sheet 3 of 5)

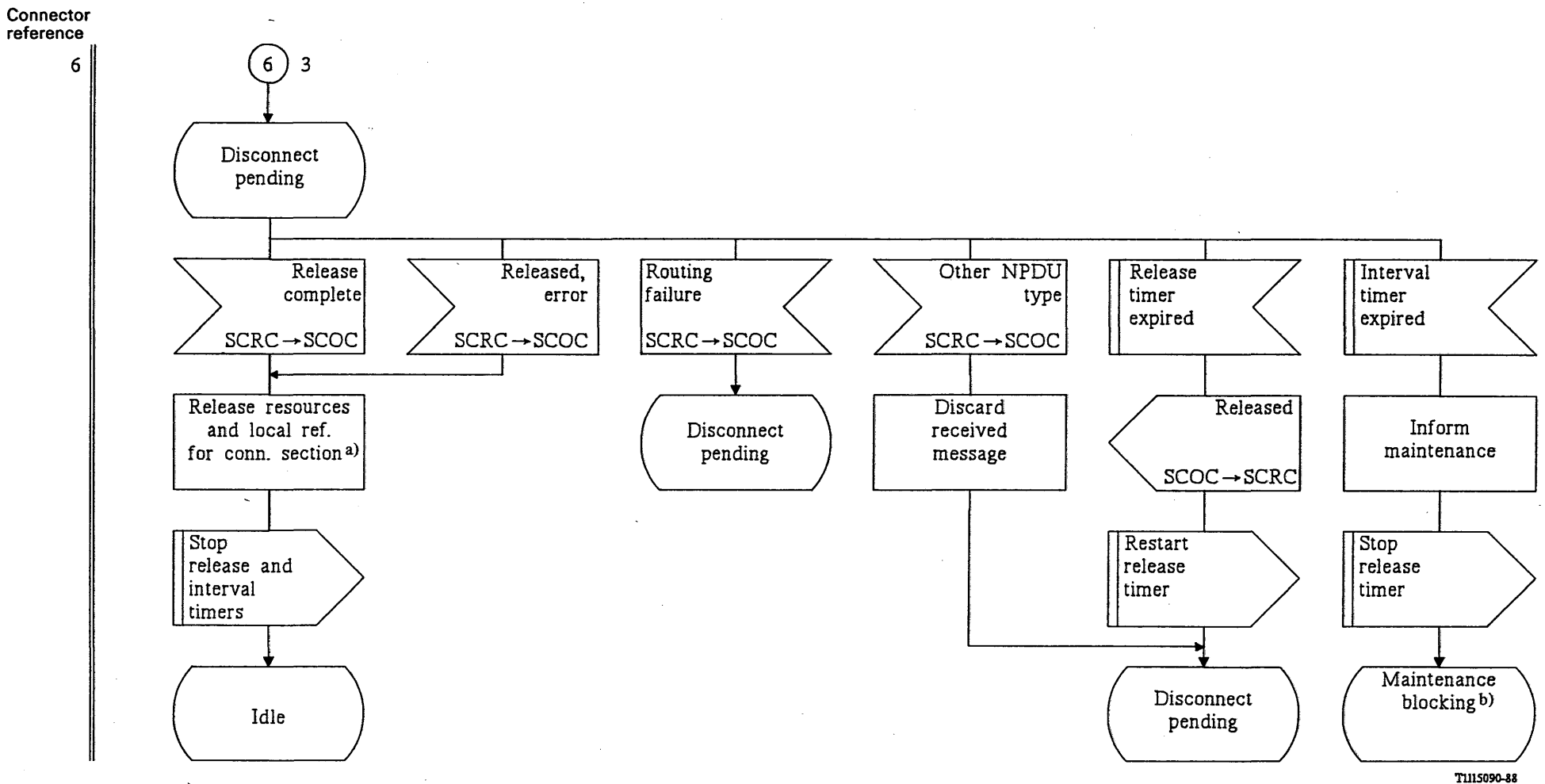
**Connection release procedures at destination node for SCCP connection-oriented control (SCOC)**




a) Freeze local reference.

FIGURE C-3/Q.714 (Sheet 4 of 5)

**Connection release procedures at destination node for SCCP connection-oriented control (SCOC)**

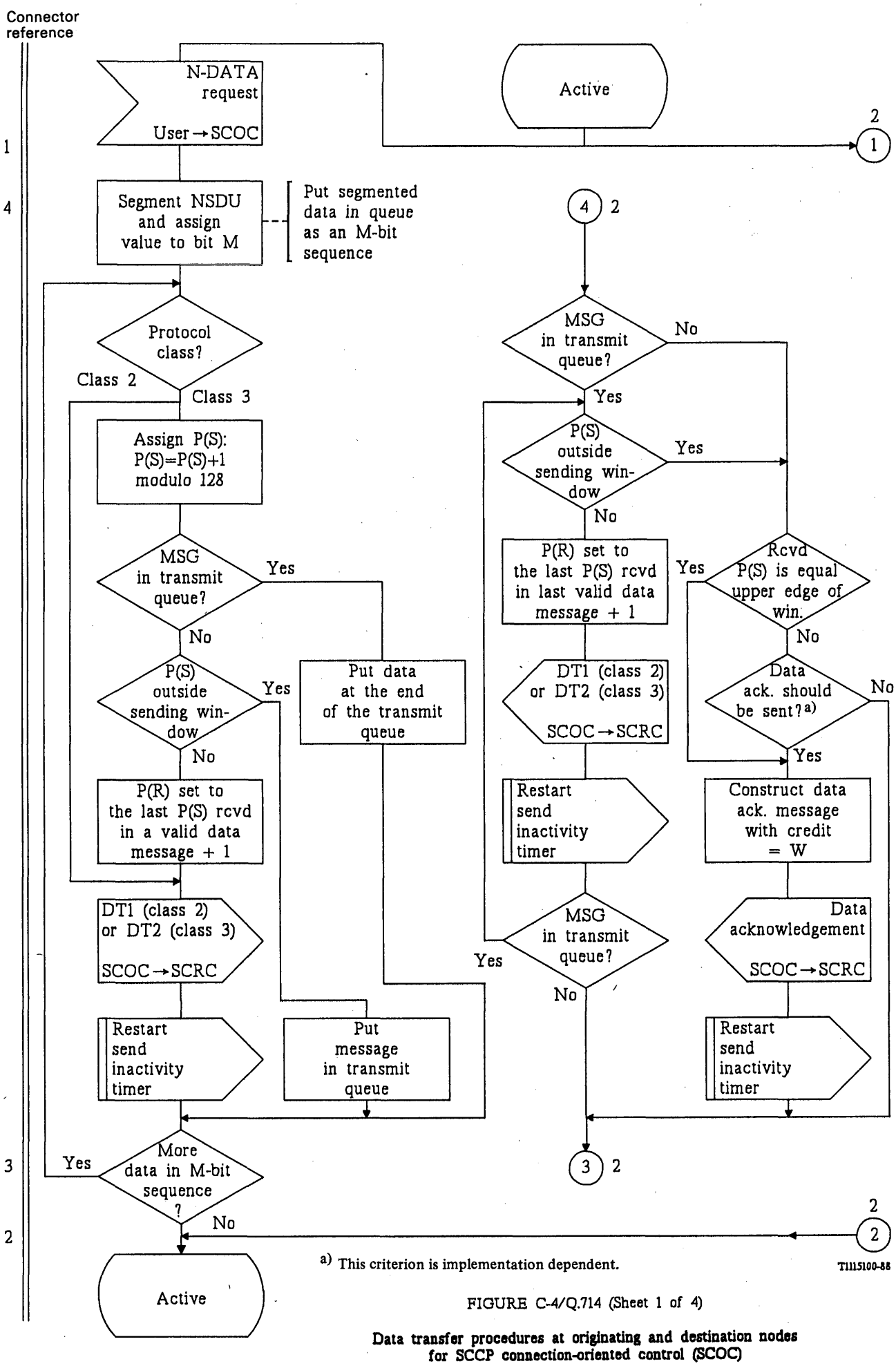



a) Freeze local reference.

b) Maintenance functions are for further study.

FIGURE C-3/Q.714 (Sheet 5 of 5)

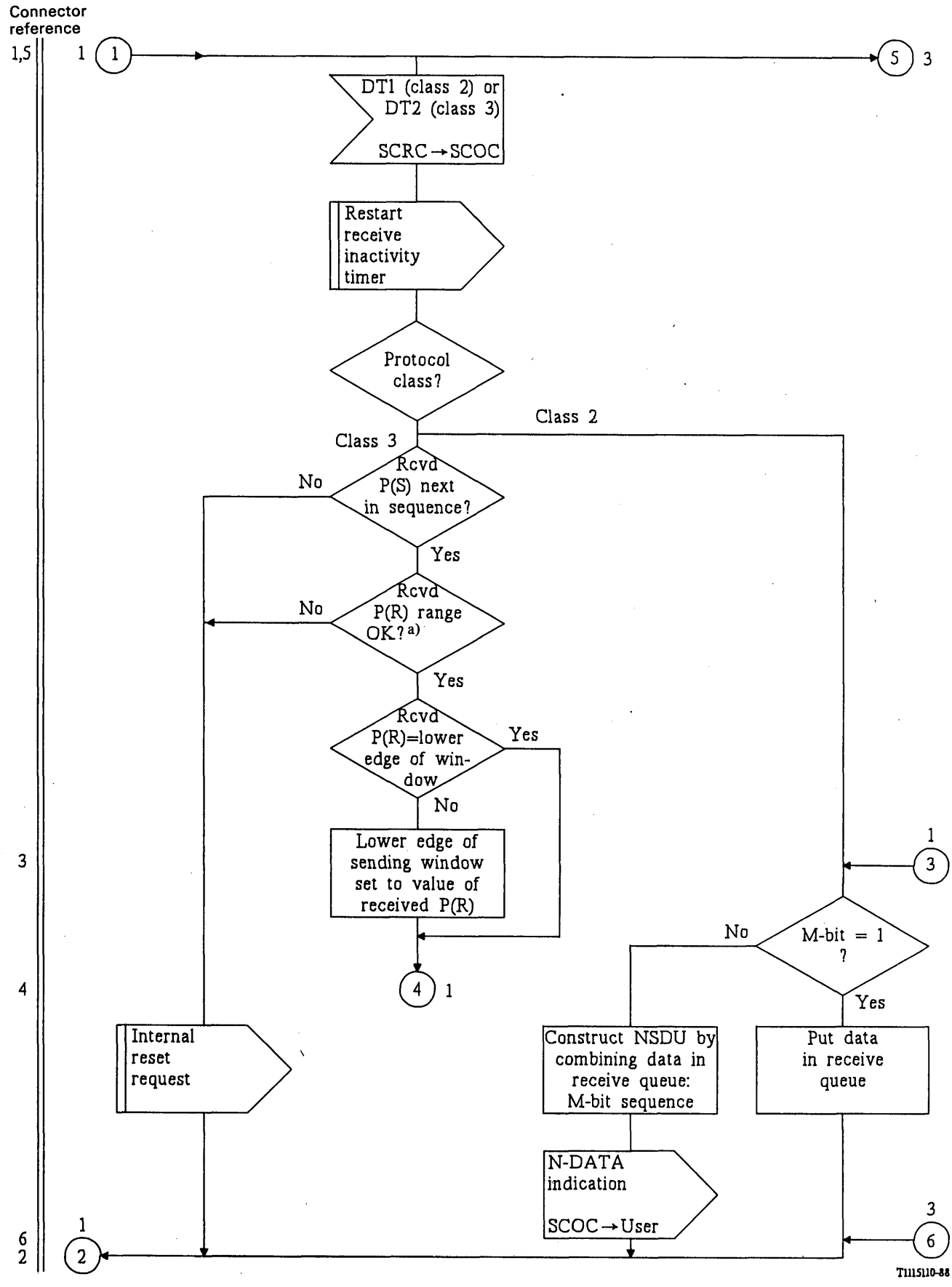
**Connection release procedures at destination node for SCCP connection-oriented control (SCOC)**




a) This criterion is implementation dependent.

FIGURE C-4/Q.714 (Sheet 1 of 4)

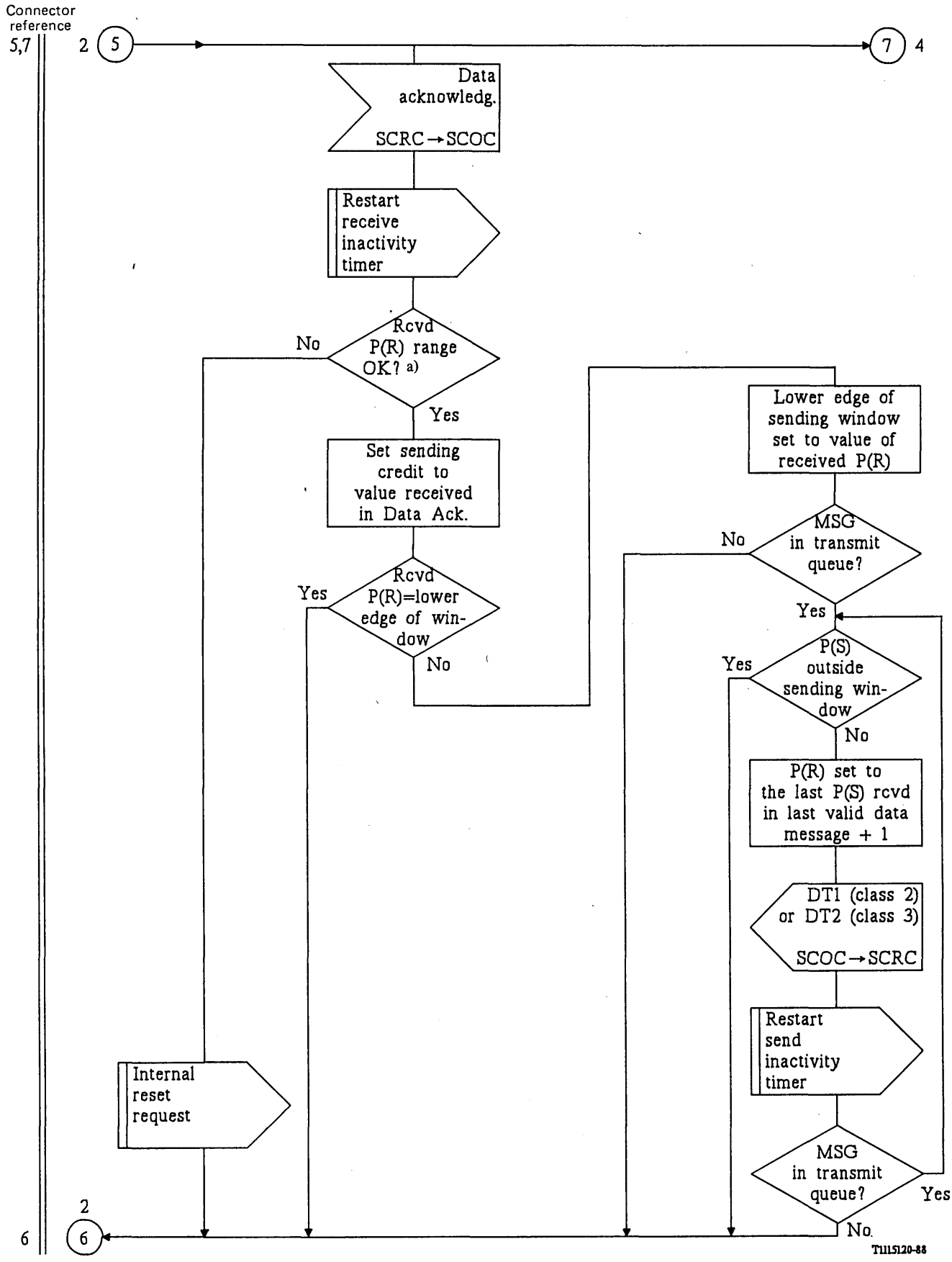
**Data transfer procedures at originating and destination nodes for SCCP connection-oriented control (SCOC)**




a) Value of P(R) received must be within the range from the last P(R) received up to including the send sequence number of next message to be transmitted.

FIGURE C-4/Q.714 (Sheet 2 of 4)

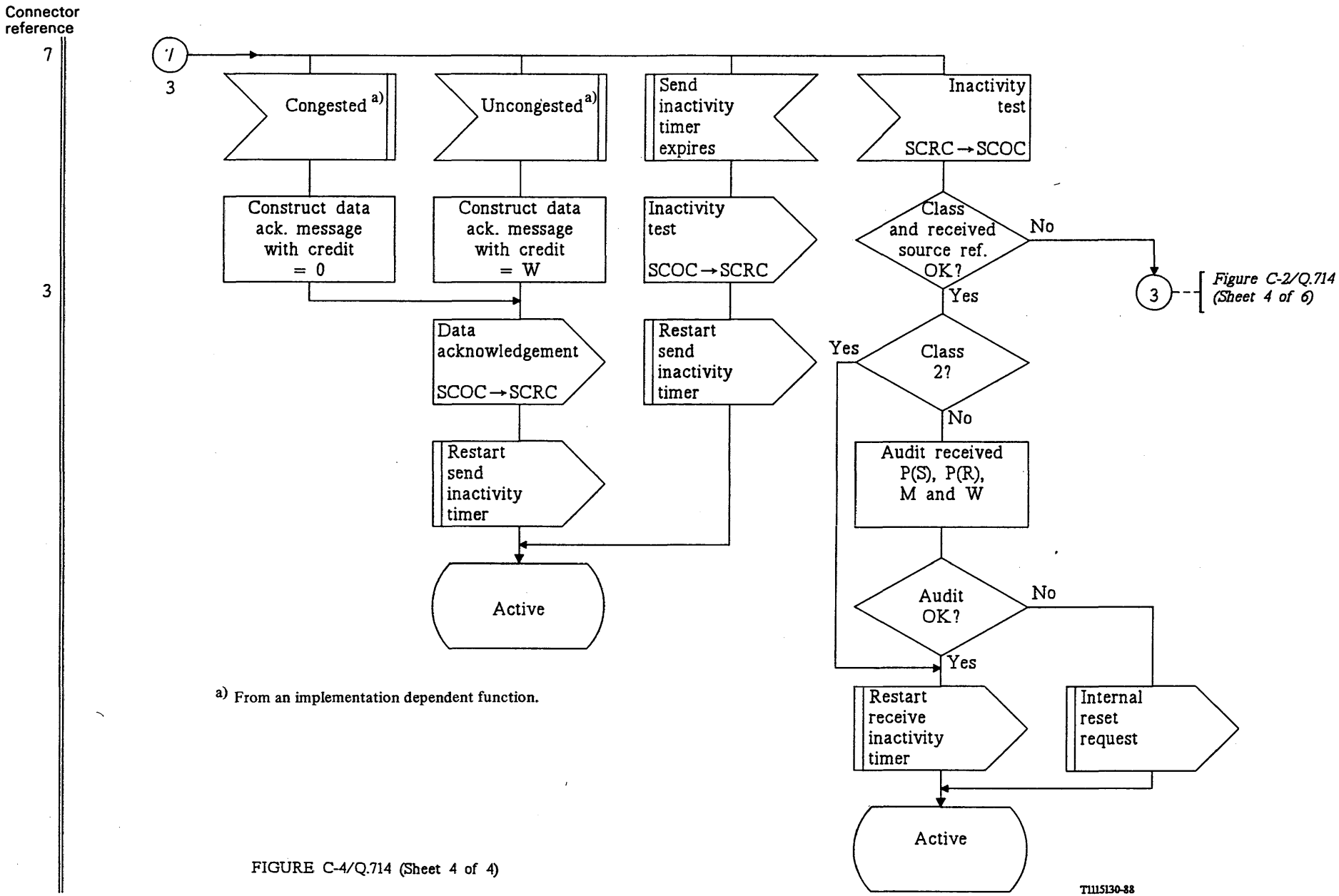
**Data transfer procedures at originating and destination nodes for SCCP connection-oriented control (SCOC)**




a) Value of P(R) received must be within the range from the last P(R) received up to including the send sequence number of next message to be transmitted.

FIGURE C-4/Q.714 (Sheet 3 of 4)

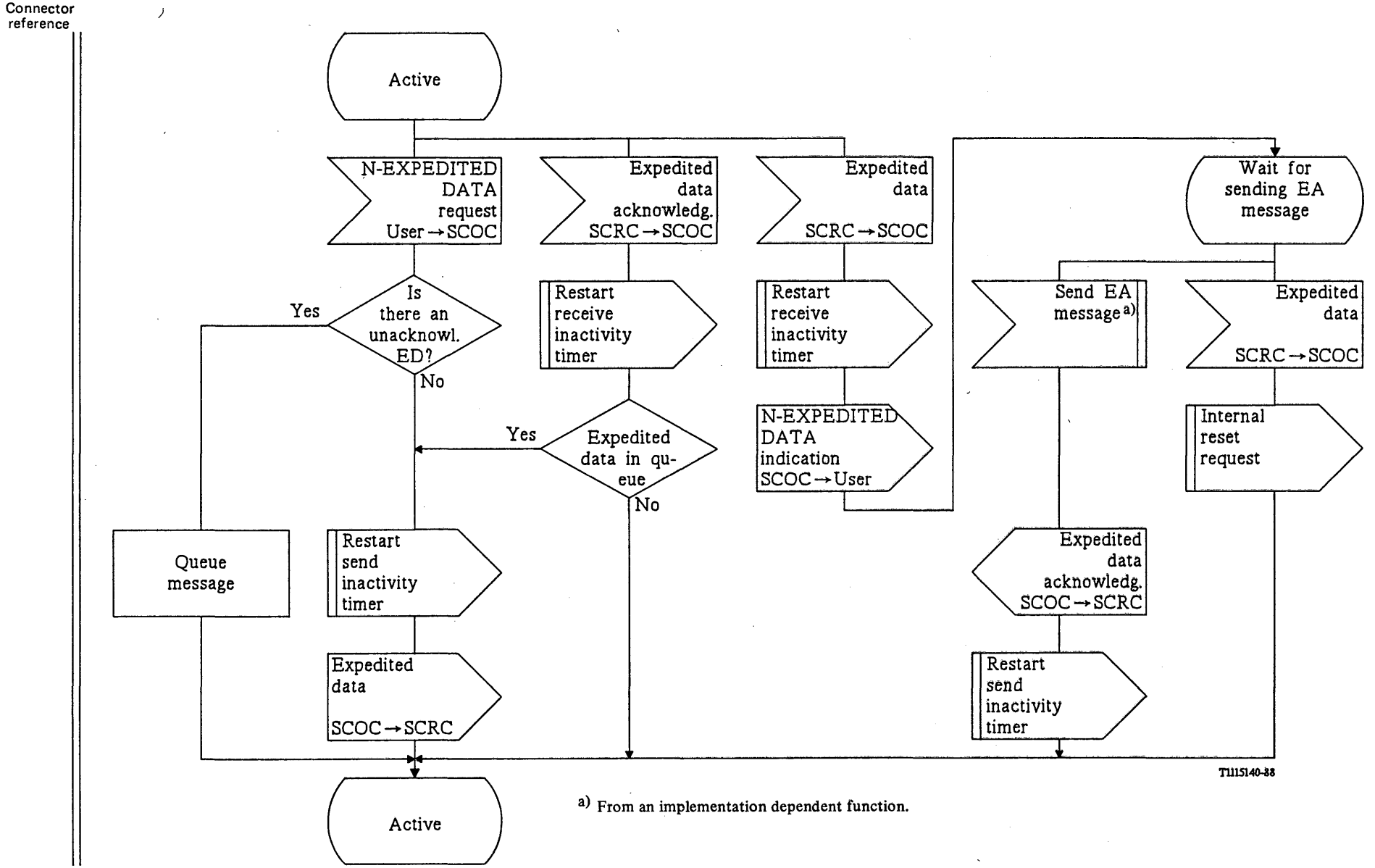
**Data transfer procedures at originating and destination nodes for SCCP connection-oriented control (SCOC)**




a) From an implementation dependent function.

FIGURE C-4/Q.714 (Sheet 4 of 4)

**Data transfer procedures at originating and destination nodes for SCCP connection-oriented control (SCOC)**




a) From an implementation dependent function.

FIGURE C-5/Q.714

**Expedited data transfer procedures at originating and destination node for SCCP connection-oriented control (SCOC)**

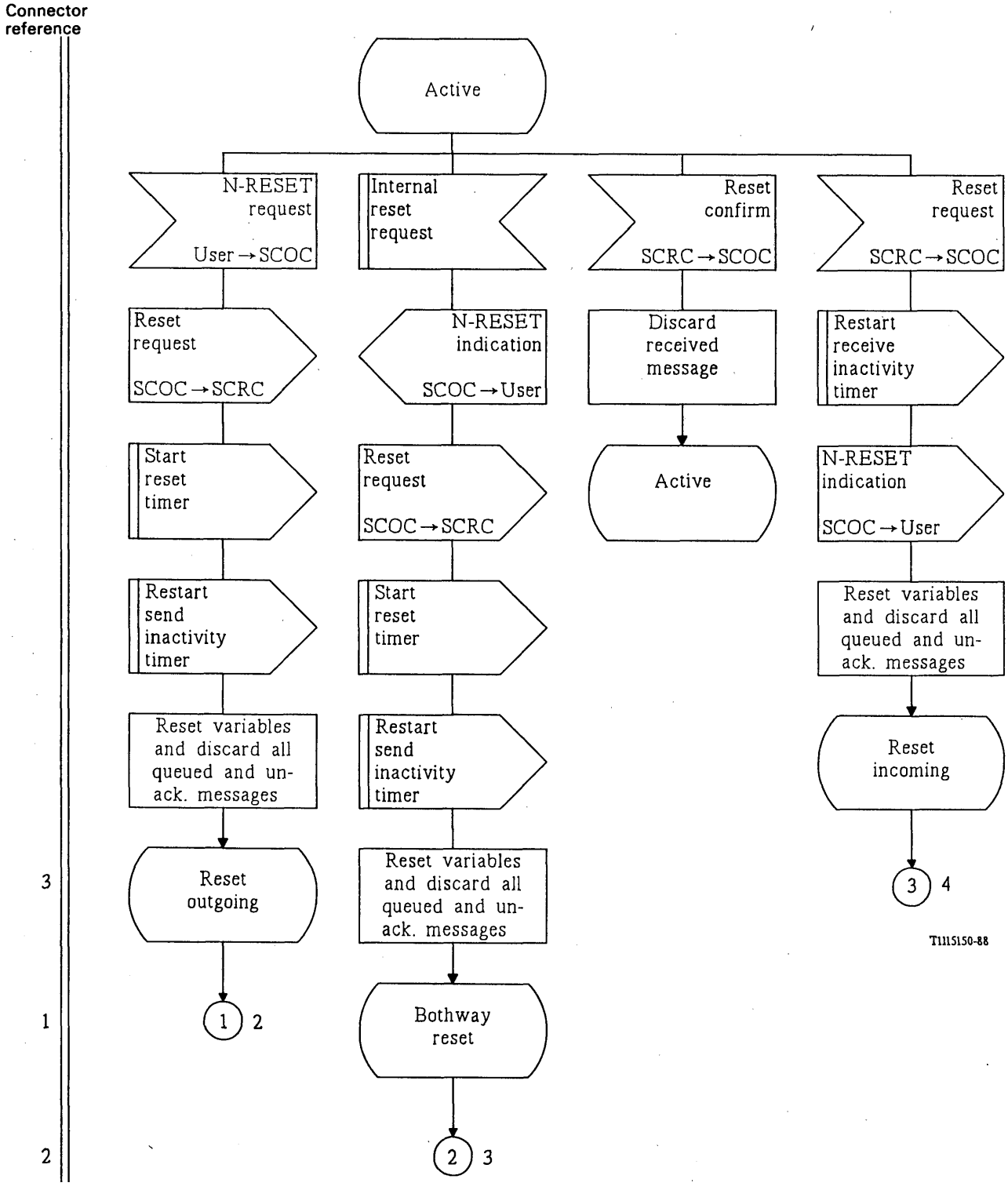



FIGURE C-6/Q.714 (Sheet 1 of 4)

**Reset procedures at originating and destination node for SCCP connection-oriented control (SCOC)**

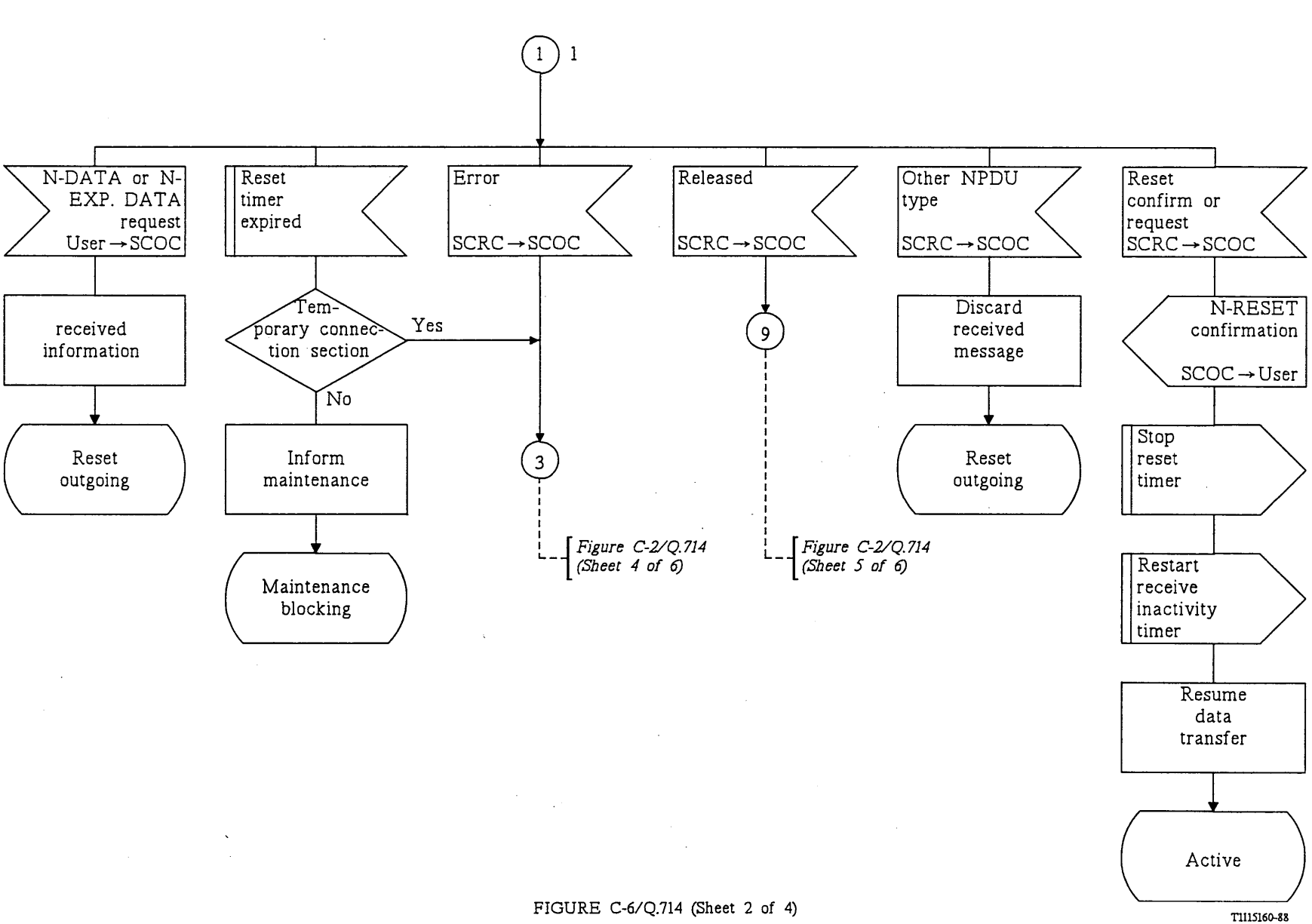



FIGURE C-6/Q.714 (Sheet 2 of 4)

**Reset procedures at originating and destination node for SCCP connection-oriented control (SCOC)**

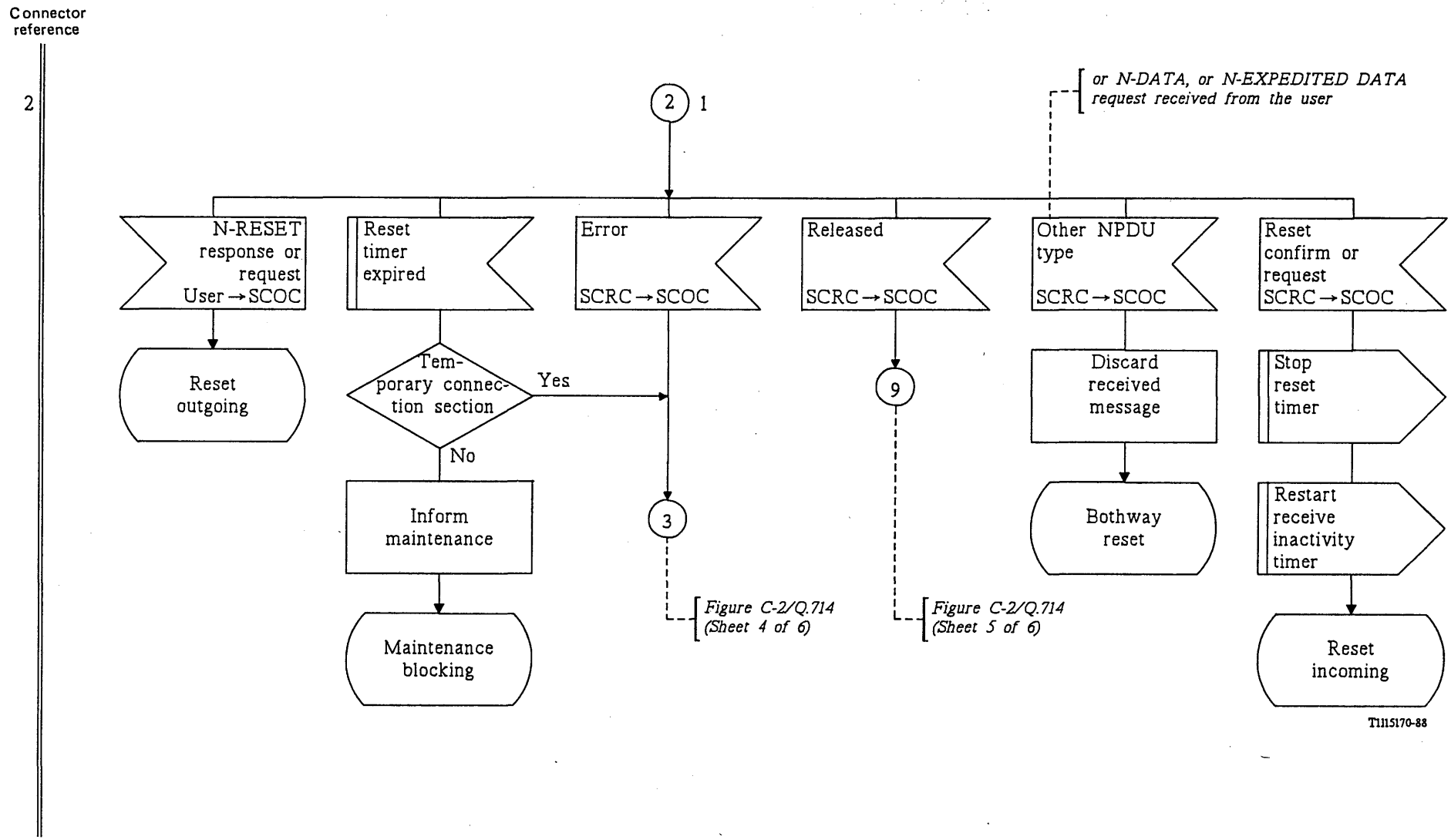



FIGURE C-6/Q.714 (Sheet 3 of 4)

**Reset procedures at originating and destination node for SCCP connection-oriented control (SCOC)**

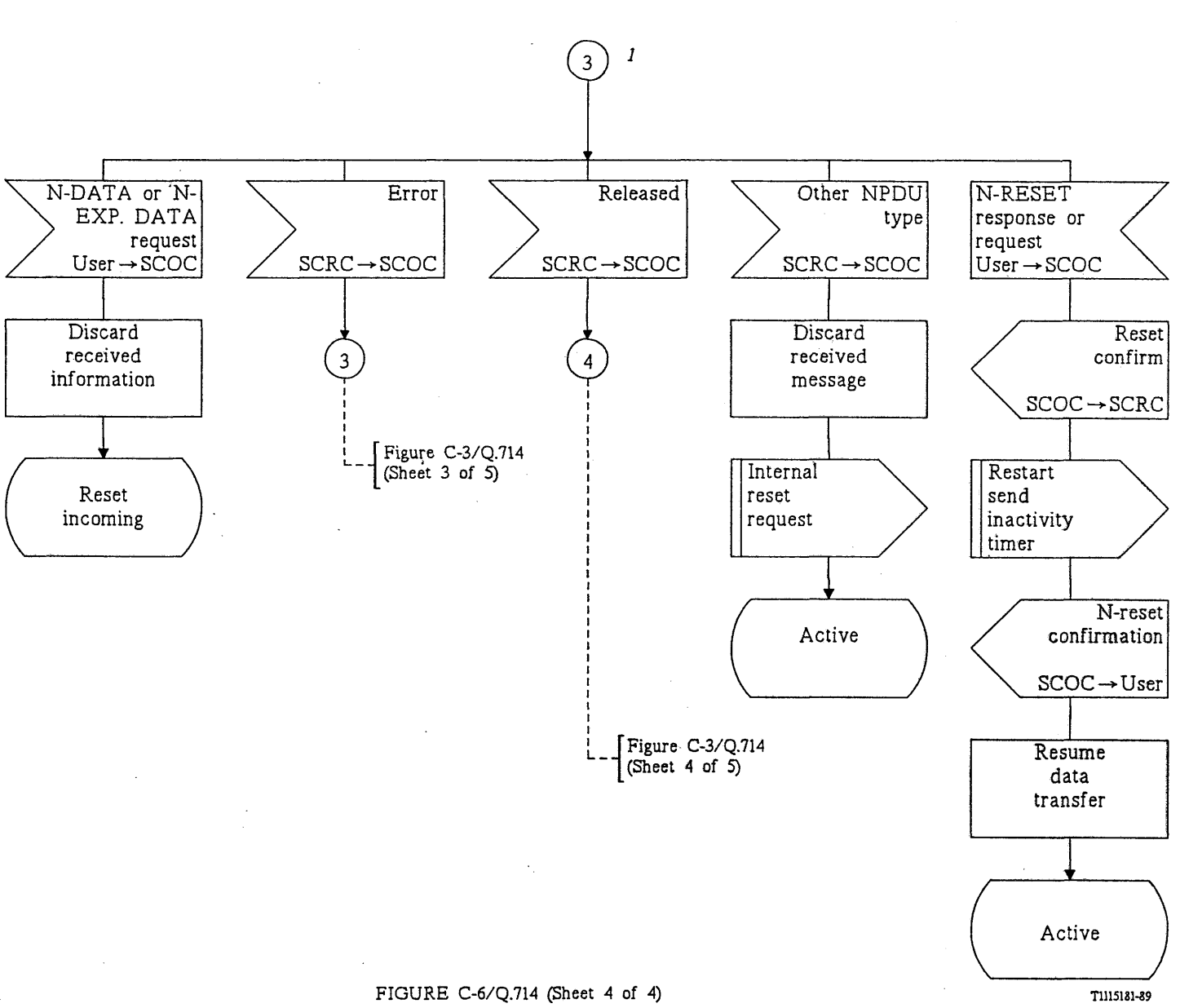
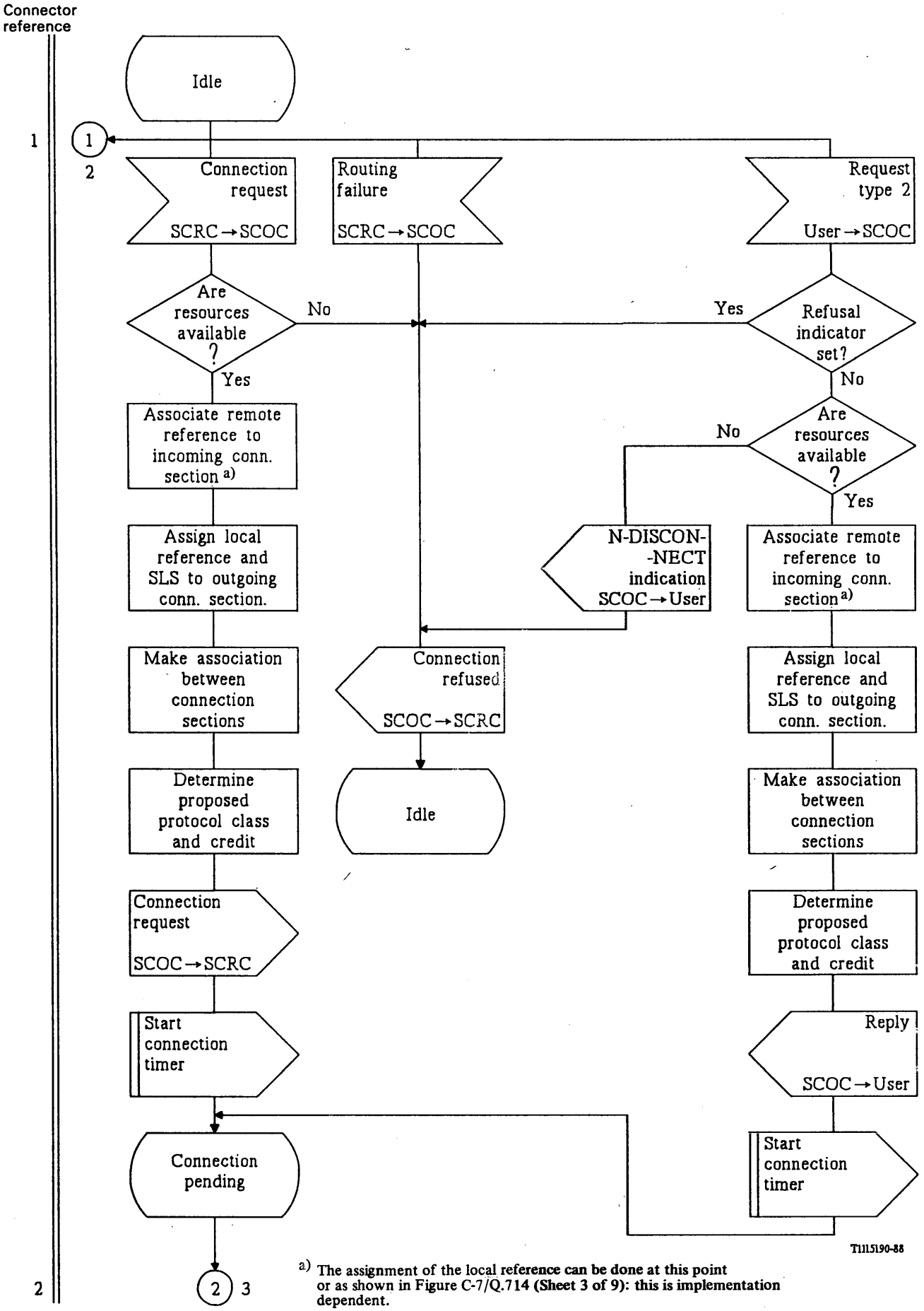



FIGURE C-6/Q.714 (Sheet 4 of 4)

**Reset procedures at originating and destination node for SCCP connection-oriented control (SCOC)**




a) The assignment of the local reference can be done at this point or as shown in Figure C-7/Q.714 (Sheet 3 of 9): this is implementation dependent.

FIGURE C-7/Q.714 (Sheet 1 of 9)

**Connection establishment procedures at the intermediate node for SCCP connection-oriented control (SCOC)**

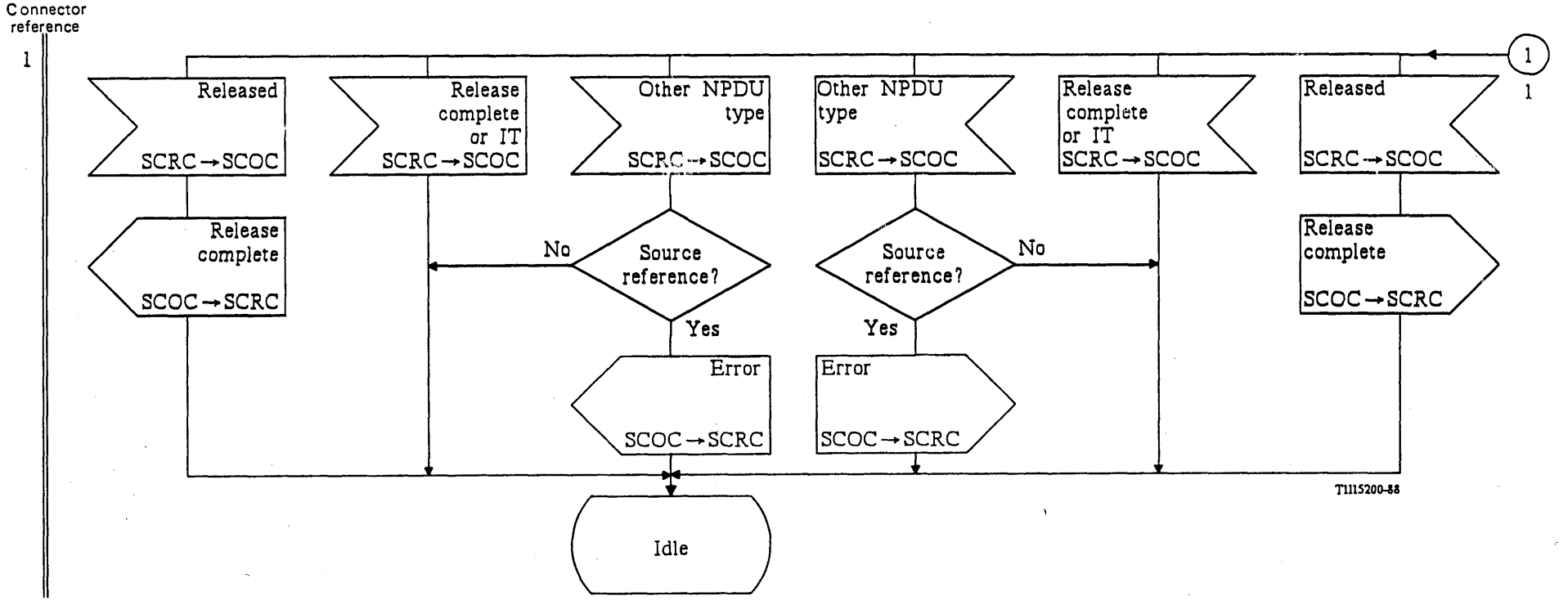
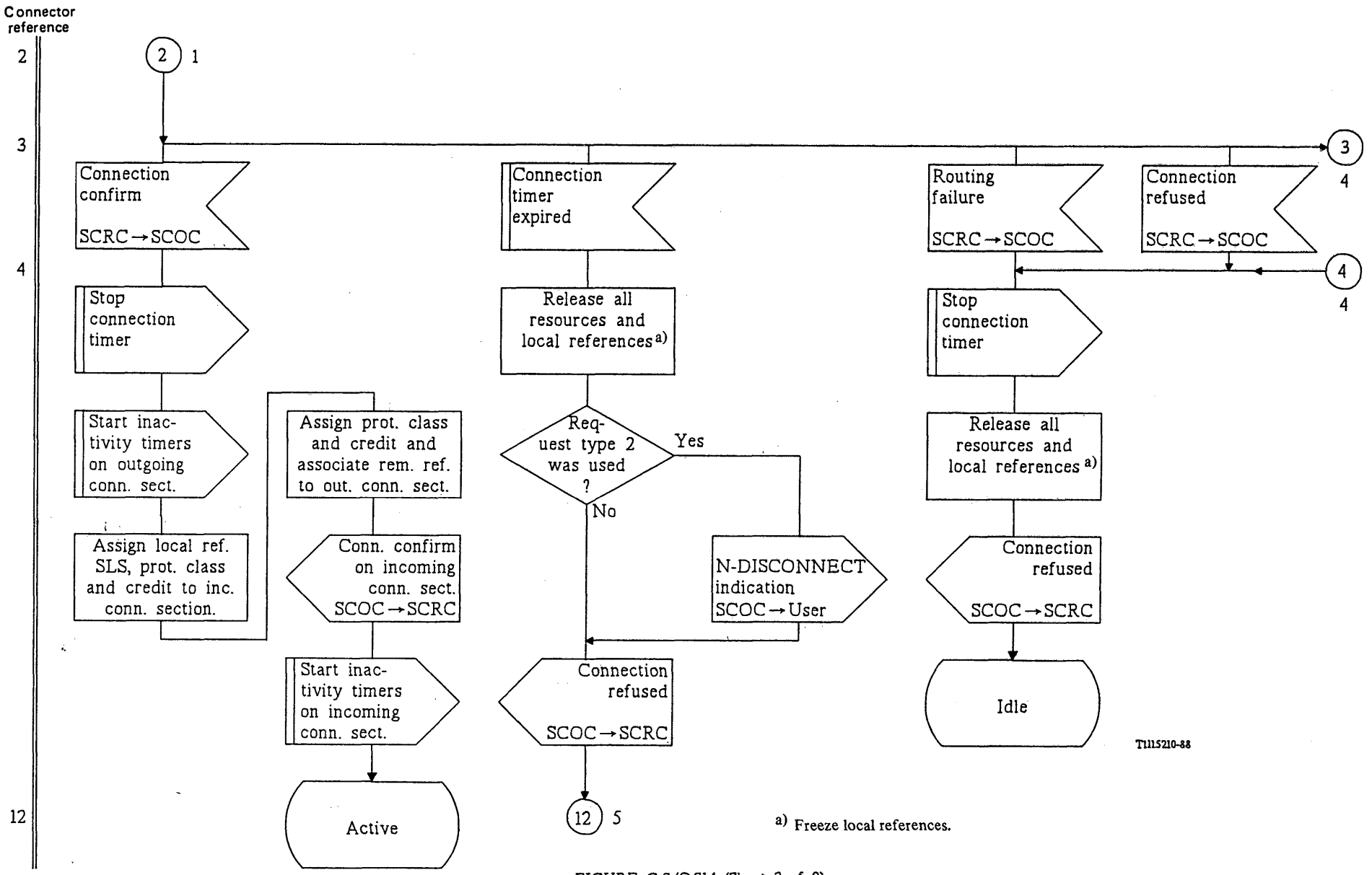



FIGURE C-7/Q.714 (Sheet 2 of 9)

**Connection establishment procedures at the intermediate node for SCCP connection-oriented control (SCOC)**




a) Freeze local references.

FIGURE C-7/Q.714 (Sheet 3 of 9)

**Connection establishment procedures at the intermediate node for SCCP connection-oriented control (SCOC)**

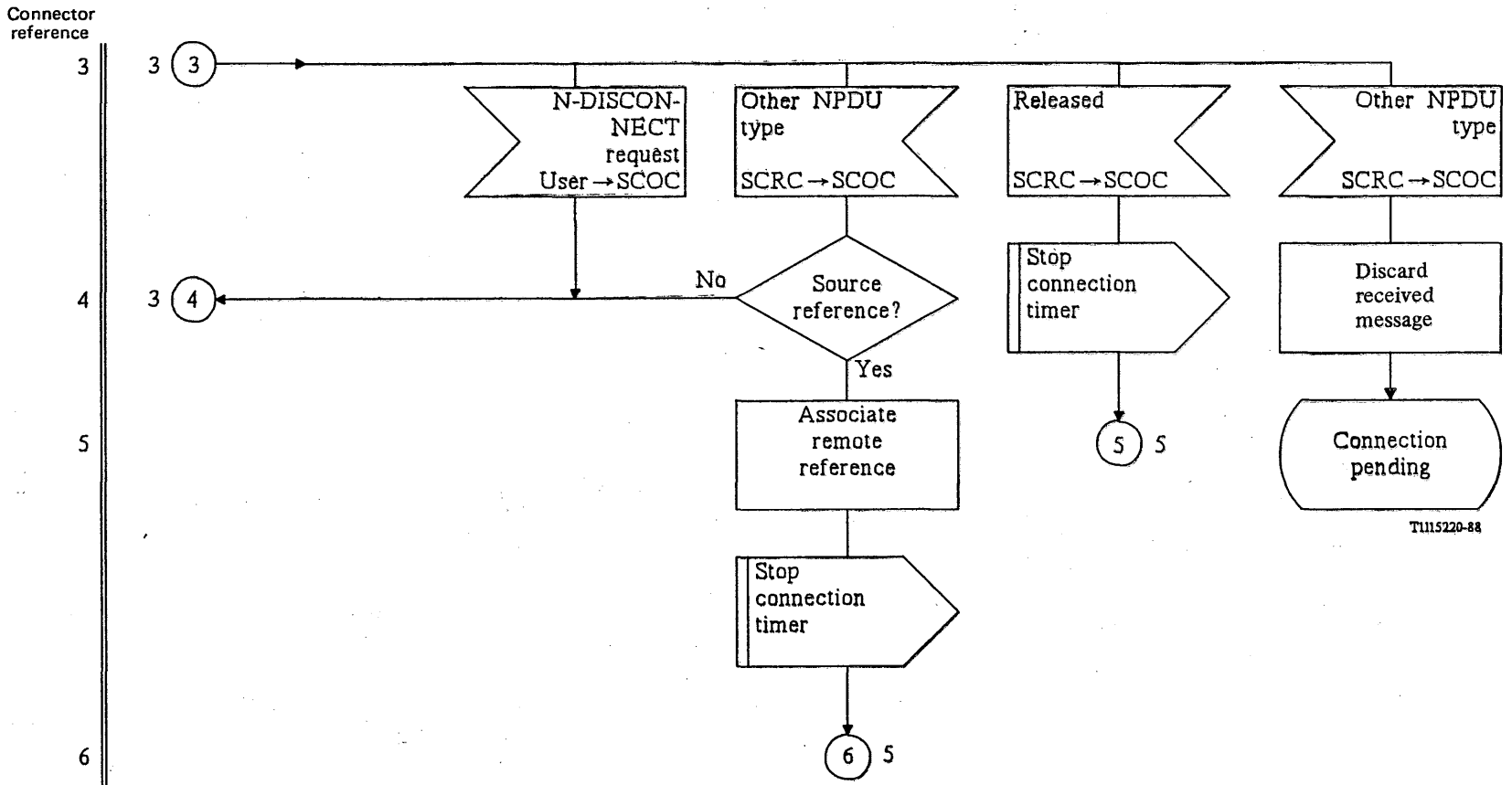
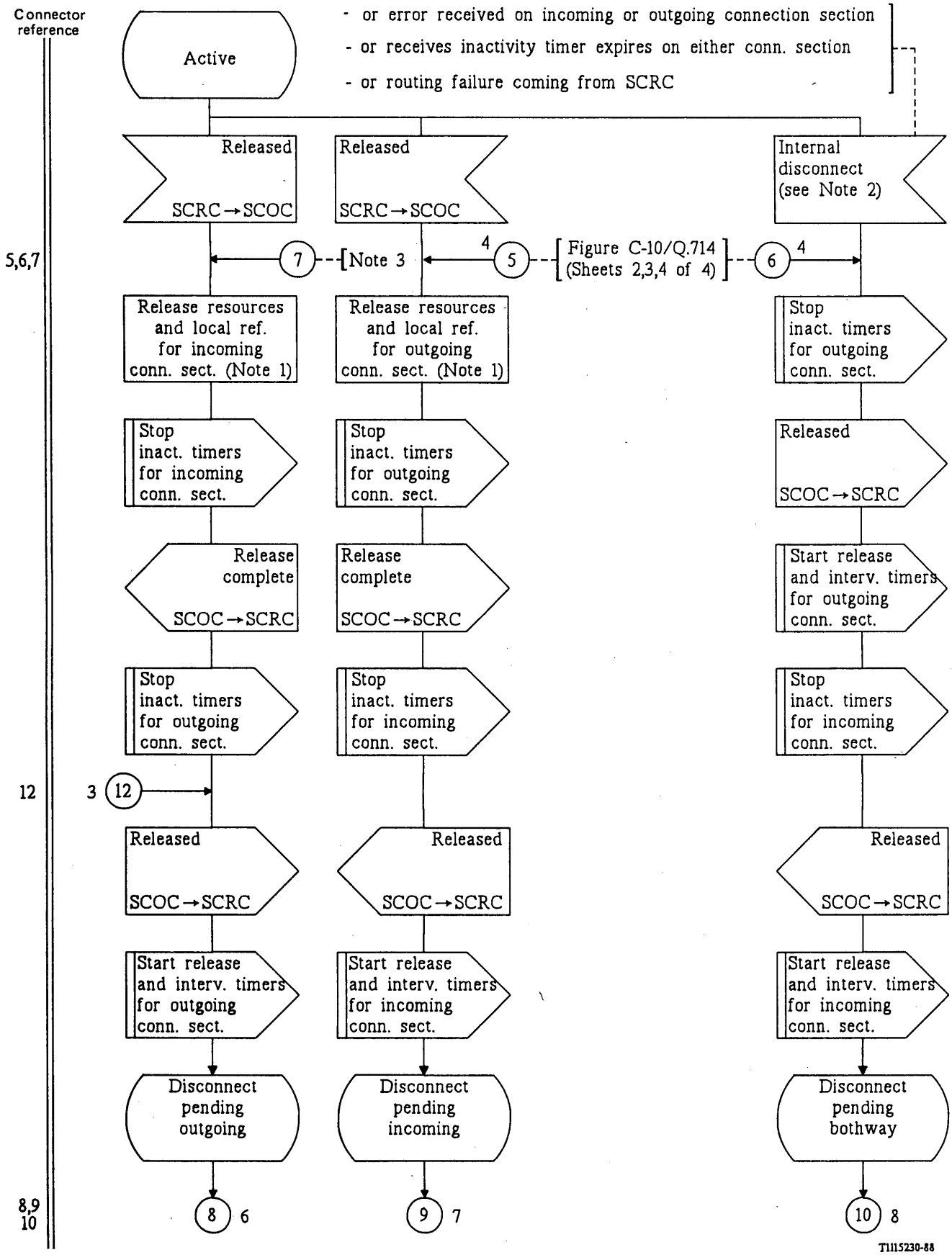



FIGURE C-7/Q.714 (Sheet 4 of 9)

**Connection establishment procedures at the intermediate node for SCCP connection-oriented control (SCOC)**




*Note 1* – Freeze local references.

*Note 2* – To cater for abnormal disconnect conditions (i.e. Table B-3/Q.714).

*Note 3* – Figure C-10/Q.714 (Sheets 2, 3, 4 of 4).

FIGURE C-7/Q.714 (Sheet 5 of 9)

**Connection release procedures at intermediate node for SCCP connection-oriented control (SCOC)**

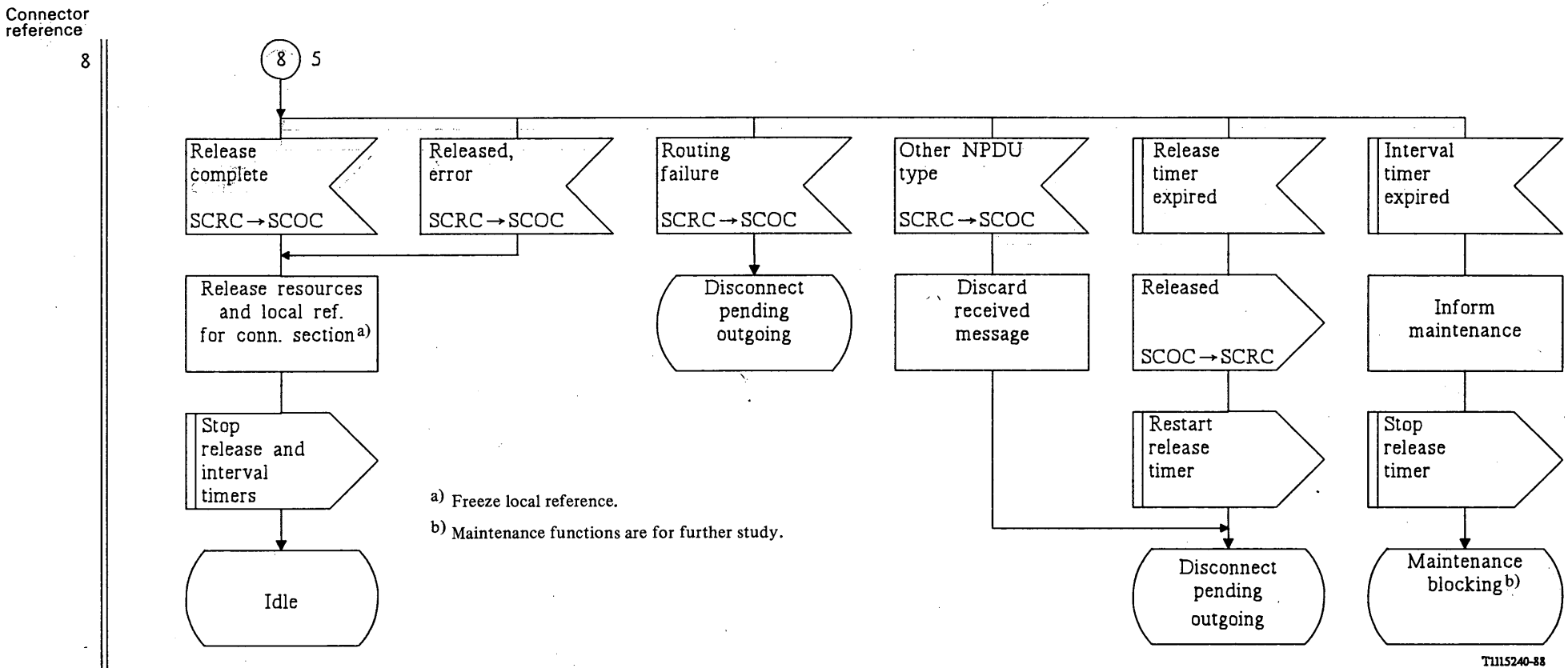
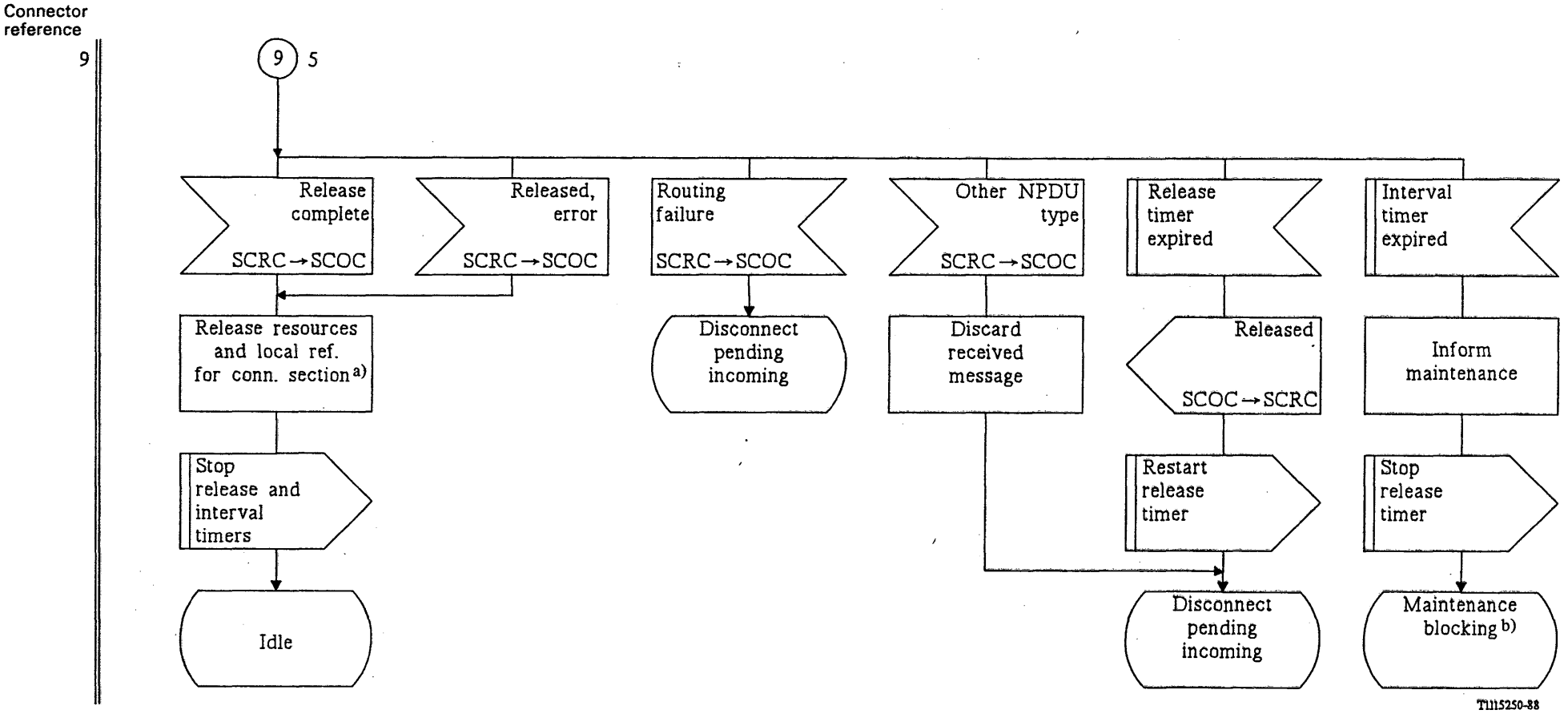



FIGURE C-7/Q.714 (Sheet 6 of 9)

**Connection release procedures at intermediate node for SCCP connection-oriented control (SCOC)**

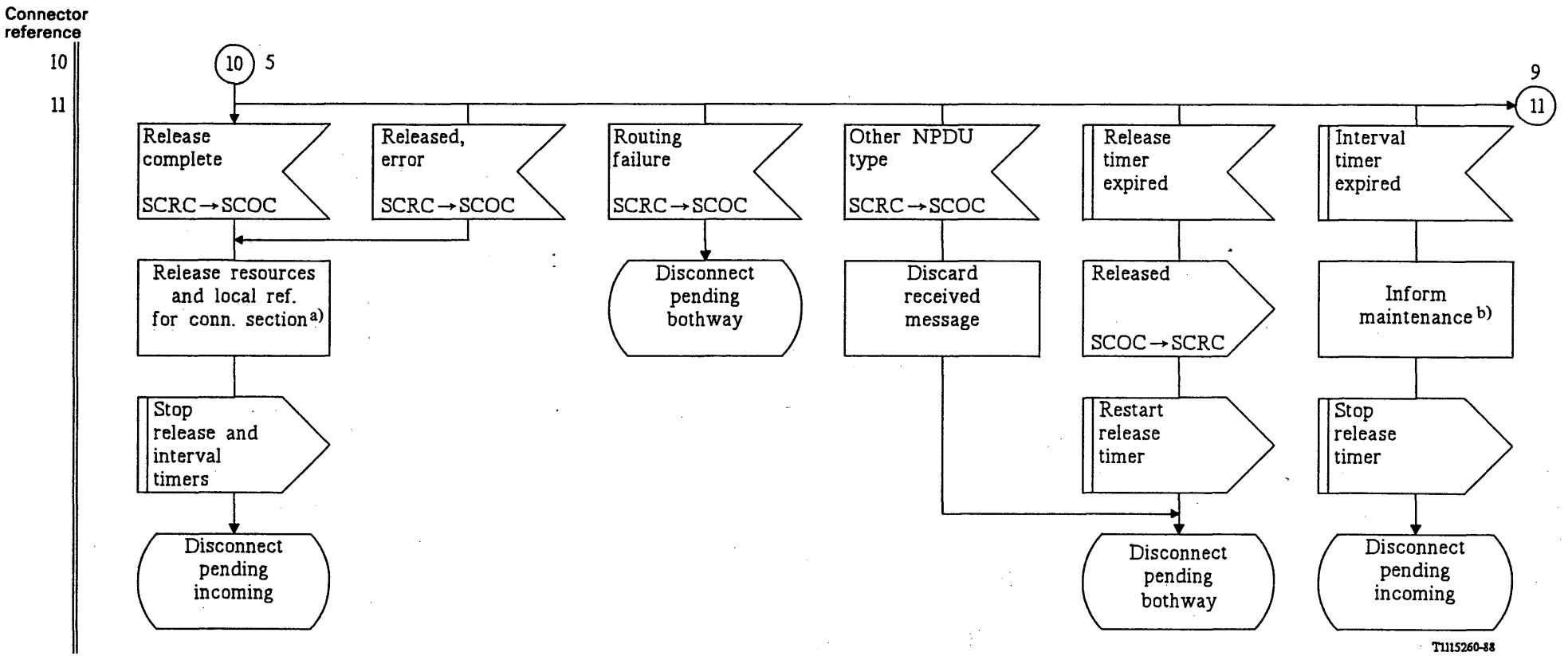



a) Freeze local reference.

b) Maintenance functions are for further study.

FIGURE C-7/Q.714 (Sheet 7 of 9)

**Connection release procedures at intermediate node for SCCP connection-oriented control (SCOC)**

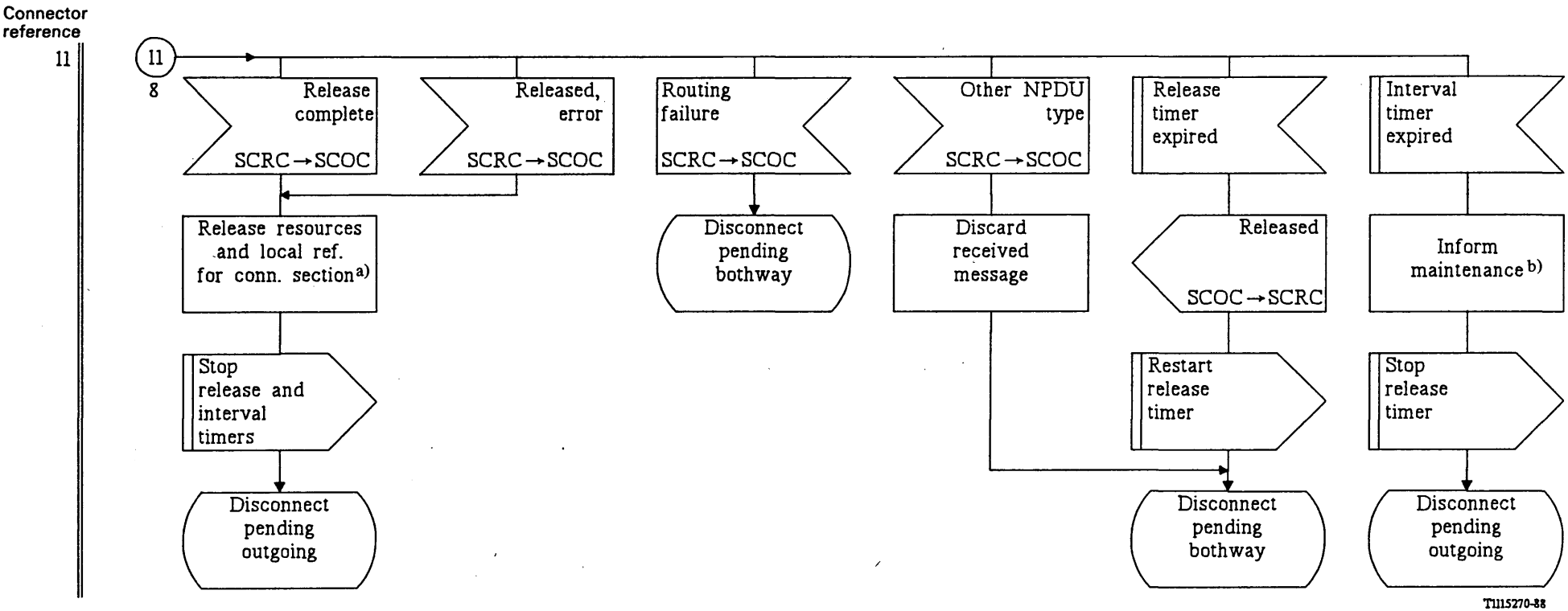



a) Freeze local reference.

b) Maintenance functions are for further study.

FIGURE C-7/Q.714 (Sheet 8 of 9)

**Connection release procedures at intermediate node for SCCP connection-oriented control (SCOC)**

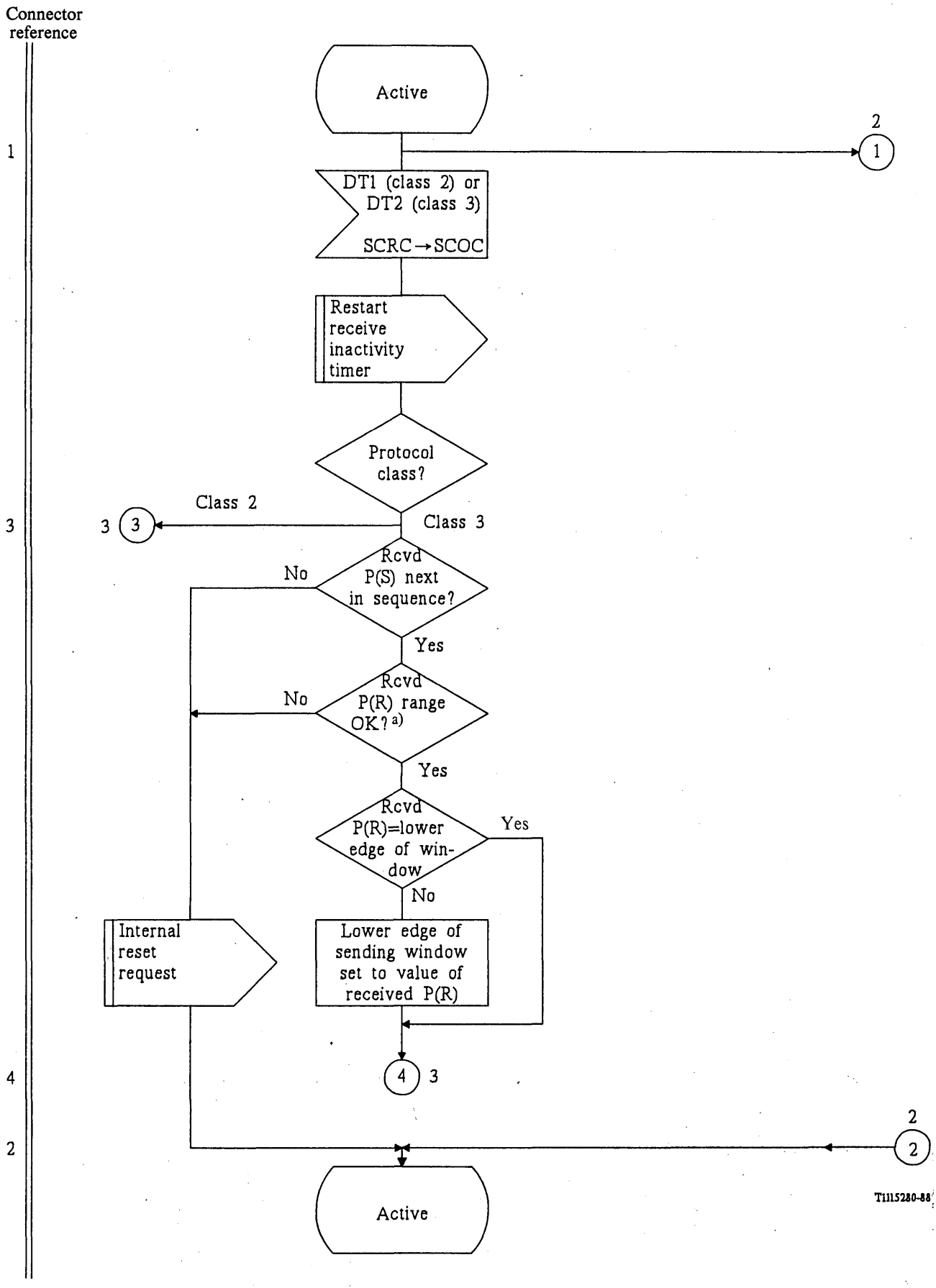



a) Freeze local reference.

b) Maintenance functions are for further study.

FIGURE C-7/Q.714 (Sheet 9 of 9)

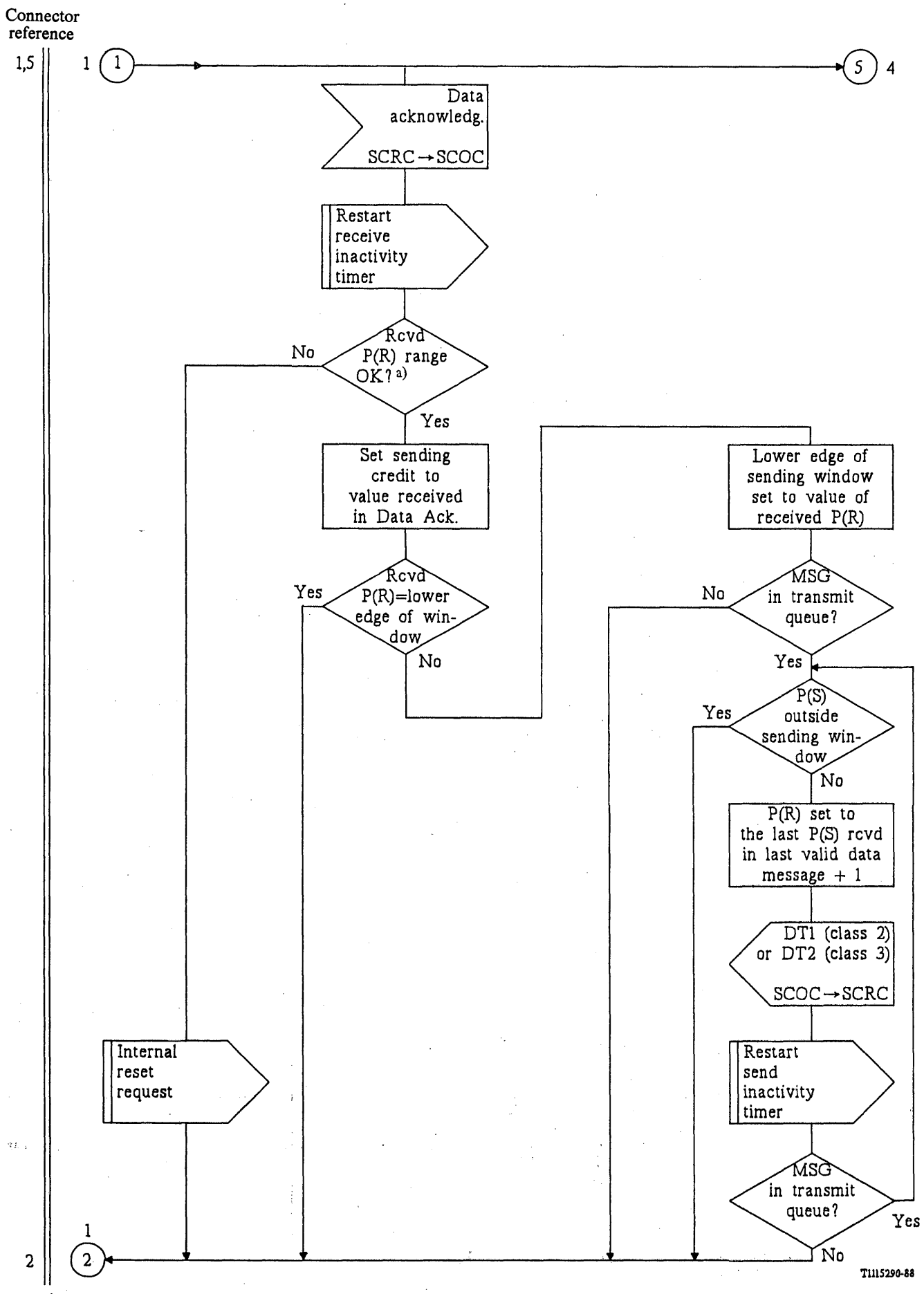
**Connection release procedures at intermediate node for SCCP connection-oriented control (SCOC)**




a) Value of P(R) received must be within the range from the last P(R) received up to including the send sequence number of next message to be transmitted.

FIGURE C-8/Q.714 (Sheet 1 of 4)

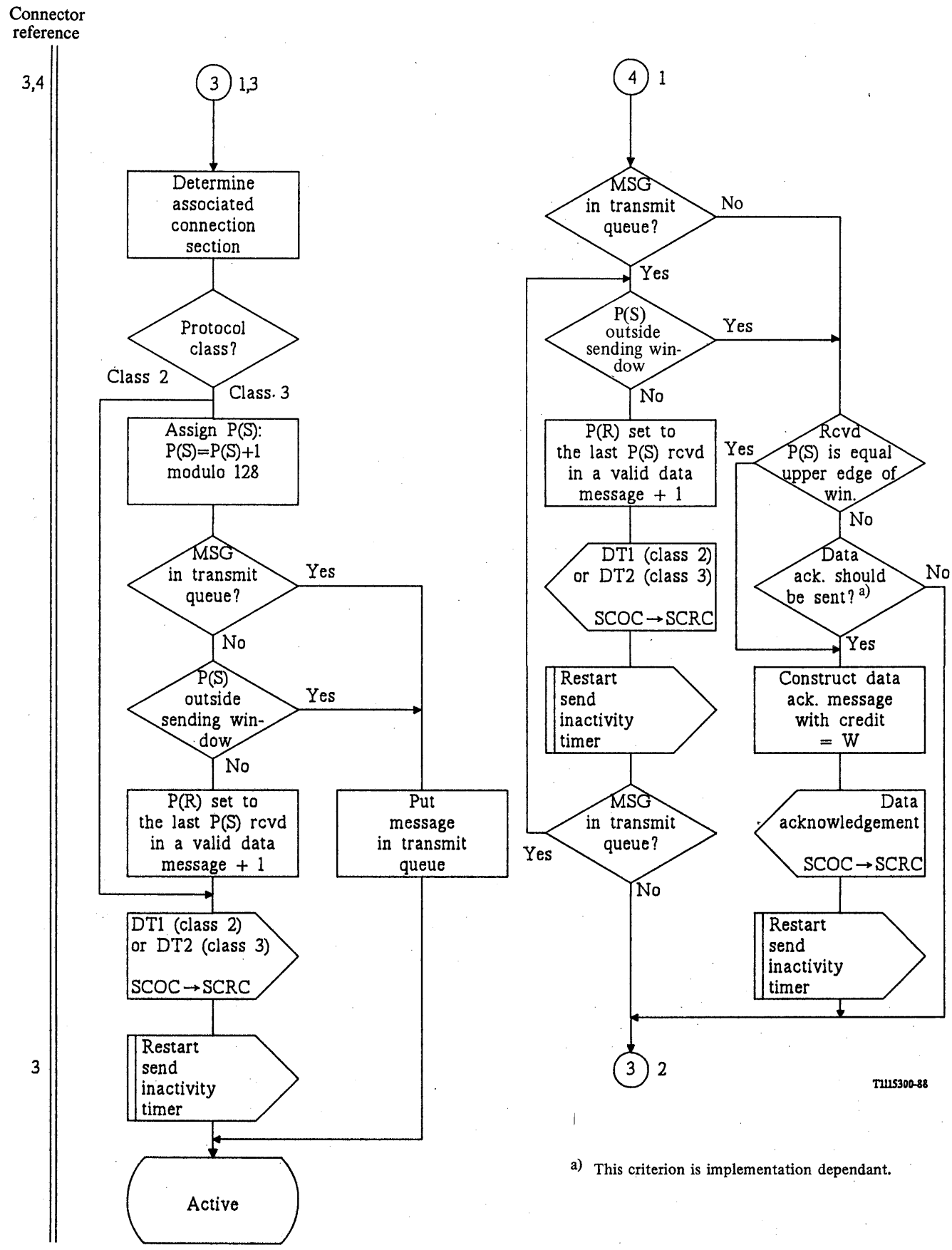
**Data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC)**




a) Value of P(R) received must be within the range from the last P(R) received up to including the send sequence number of next message to be transmitted.

FIGURE C-8/Q.714 (Sheet 2 of 4)

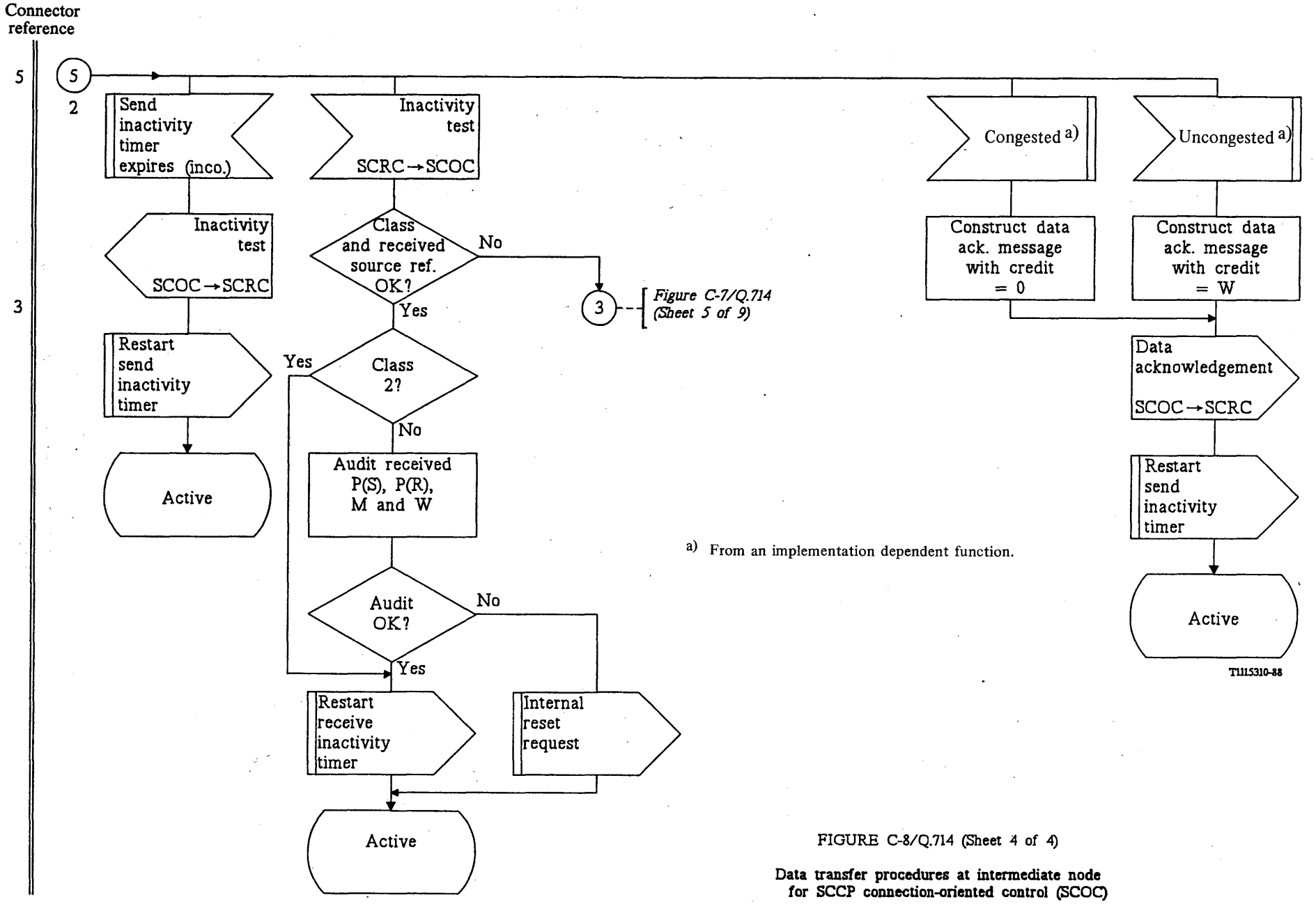
**Data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC)**




a) This criterion is implementation dependant.

FIGURE C-8/Q.714 (Sheet 3 of 4)

**Data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC)**




a) From an implementation dependent function.

FIGURE C-8/Q.714 (Sheet 4 of 4)

**Data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC)**

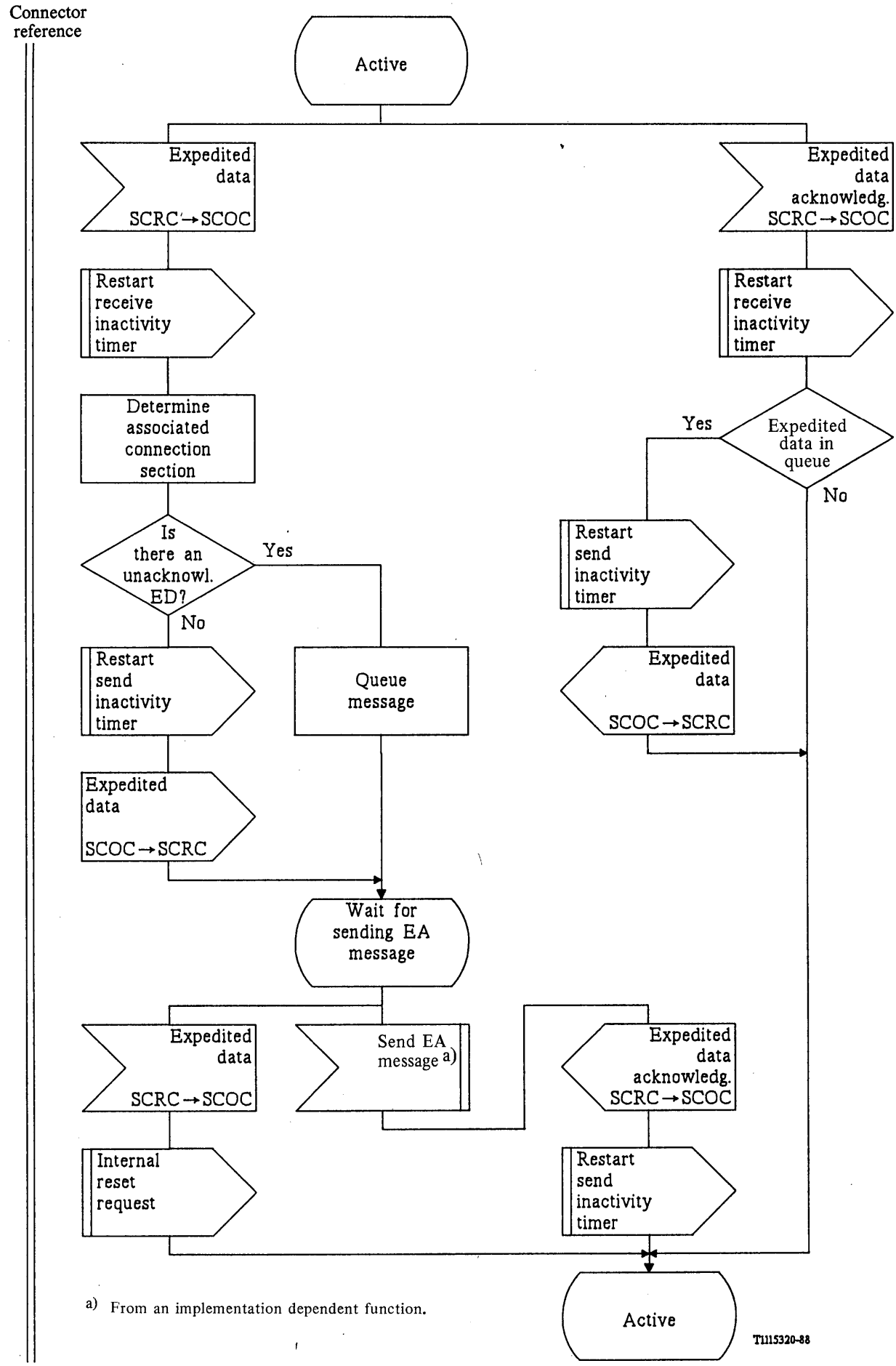



FIGURE C-9/Q.714

**Expedited data transfer procedures at intermediate node for SCCP connection-oriented control (SCOC)**

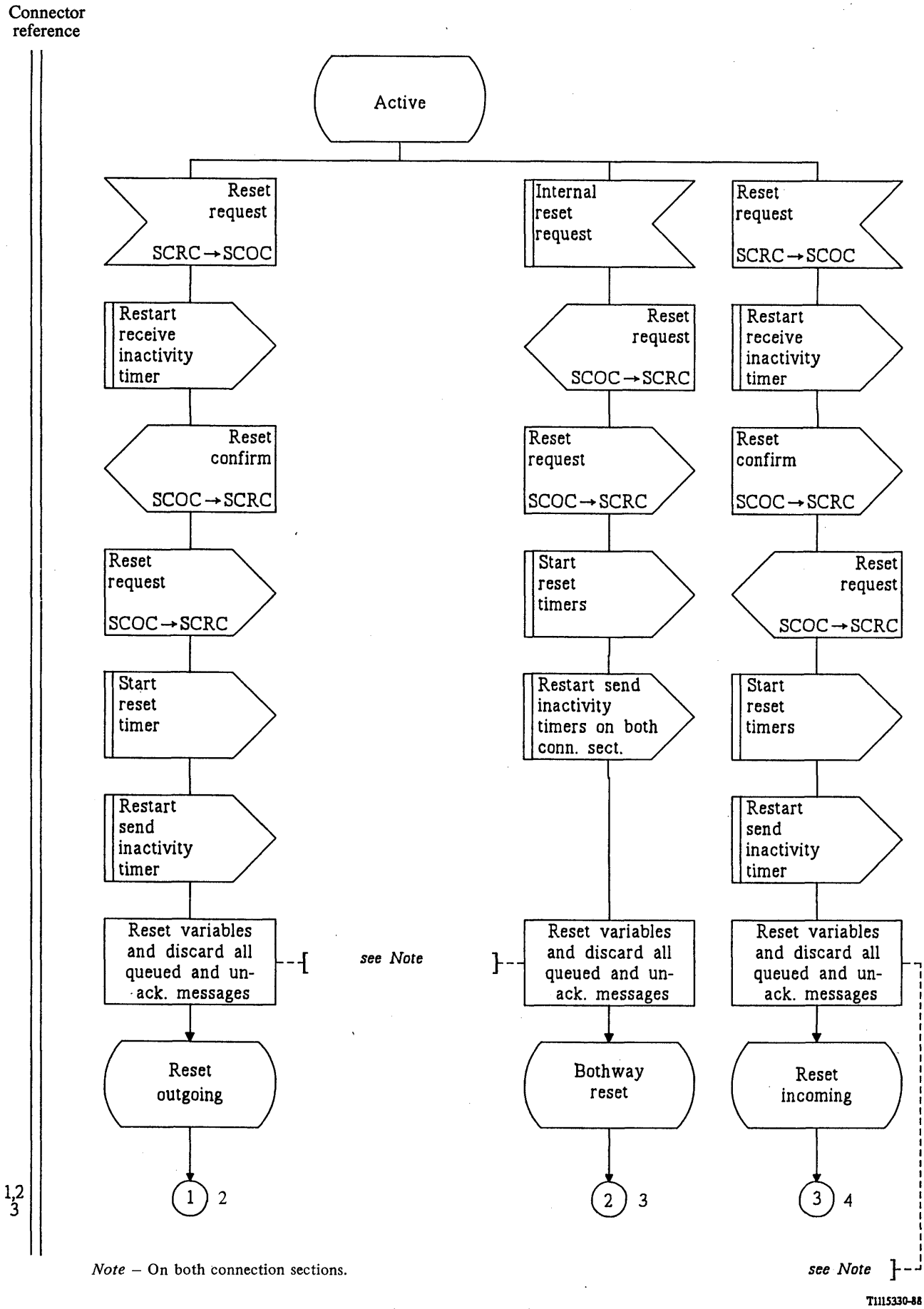



FIGURE C-10/Q.714 (Sheet 1 of 4)

**Reset procedures at intermediate node for SCCP connection-oriented control (SCOC)**

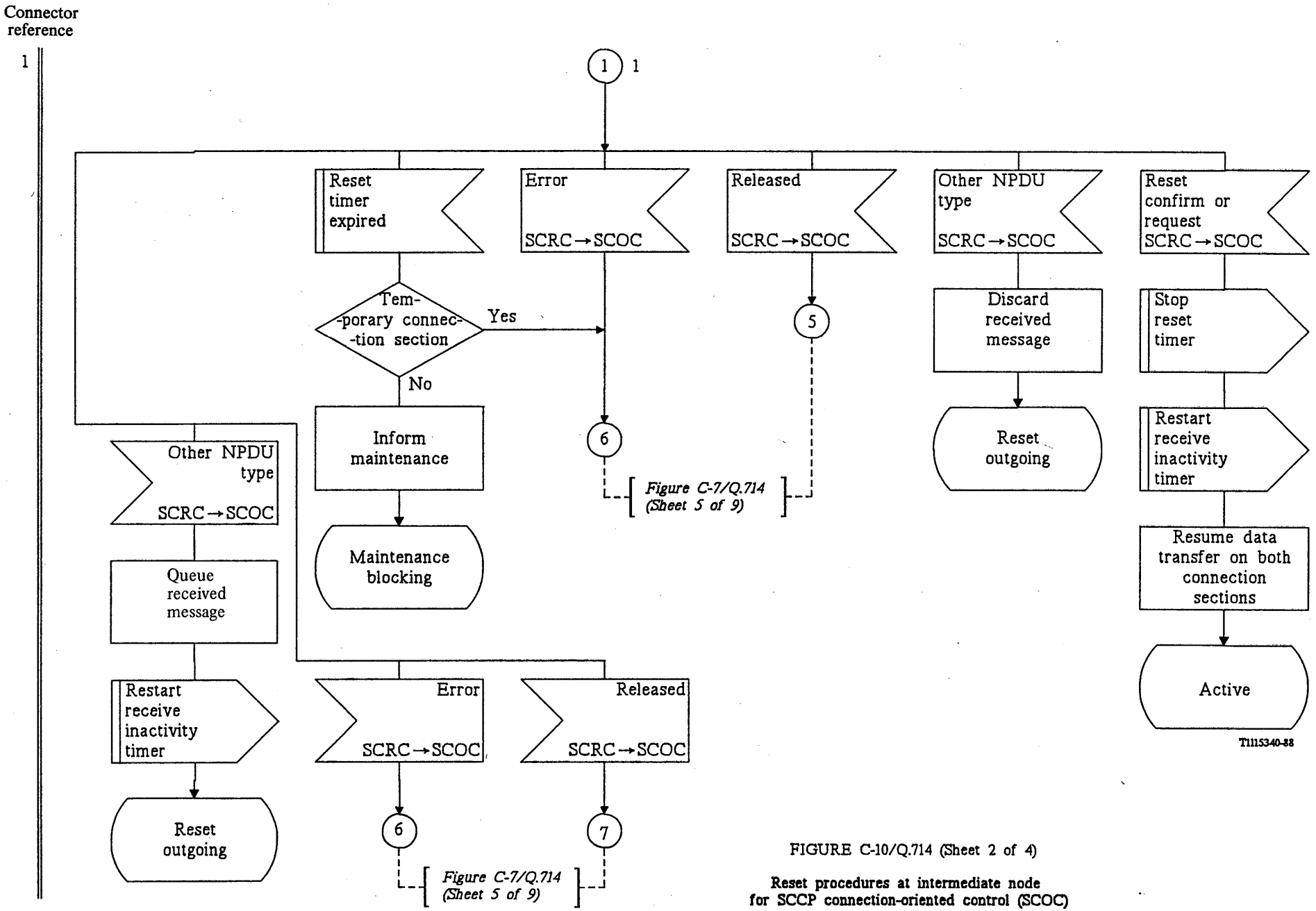



FIGURE C-10/Q.714 (Sheet 2 of 4)

**Reset procedures at intermediate node for SCCP connection-oriented control (SCOC)**

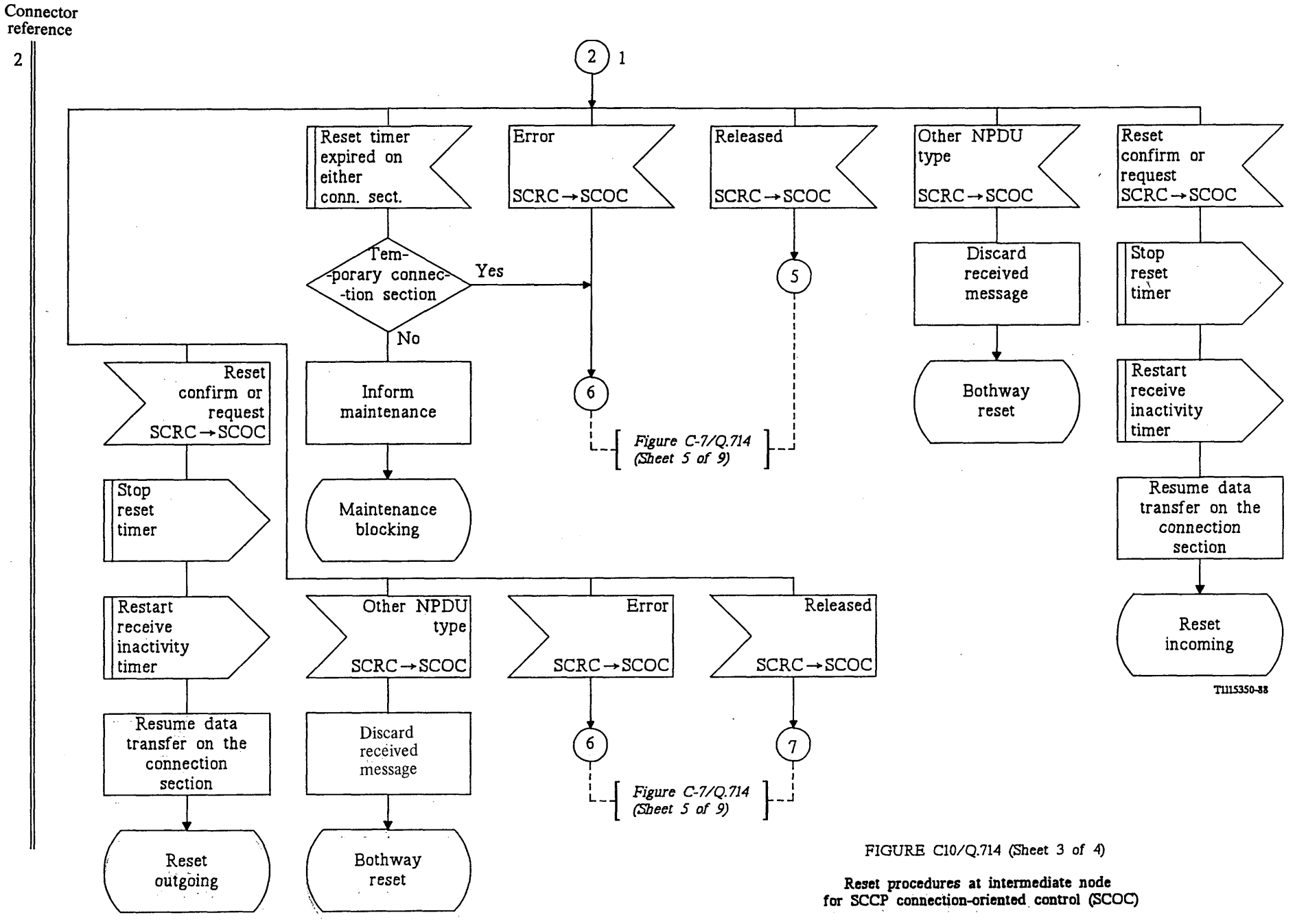



FIGURE C10/Q.714 (Sheet 3 of 4)

**Reset procedures at intermediate node for SCCP connection-oriented control (SCOC)**

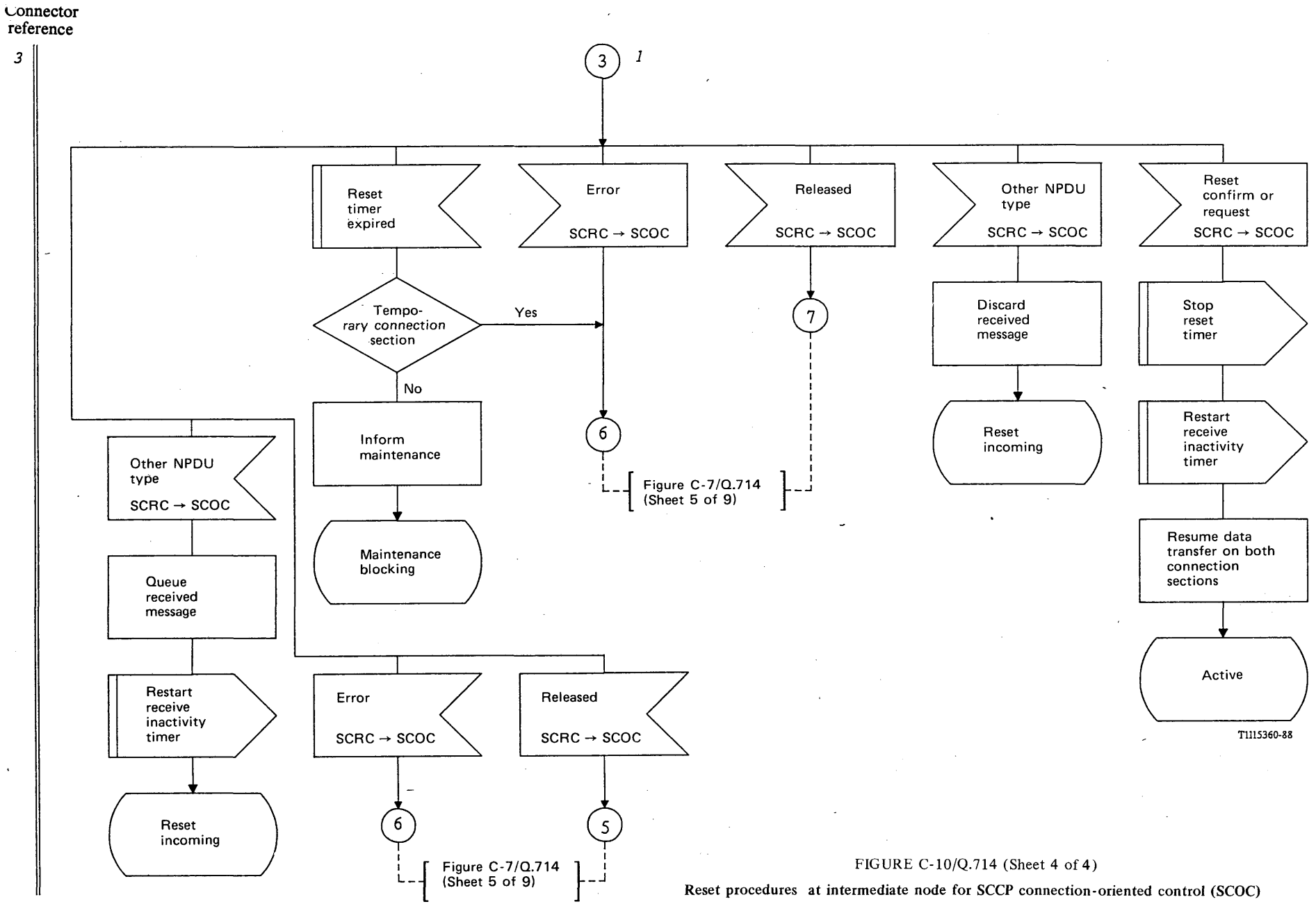



FIGURE C-10/Q.714 (Sheet 4 of 4)

**Reset procedures at intermediate node for SCCP connection-oriented control (SCOC)**

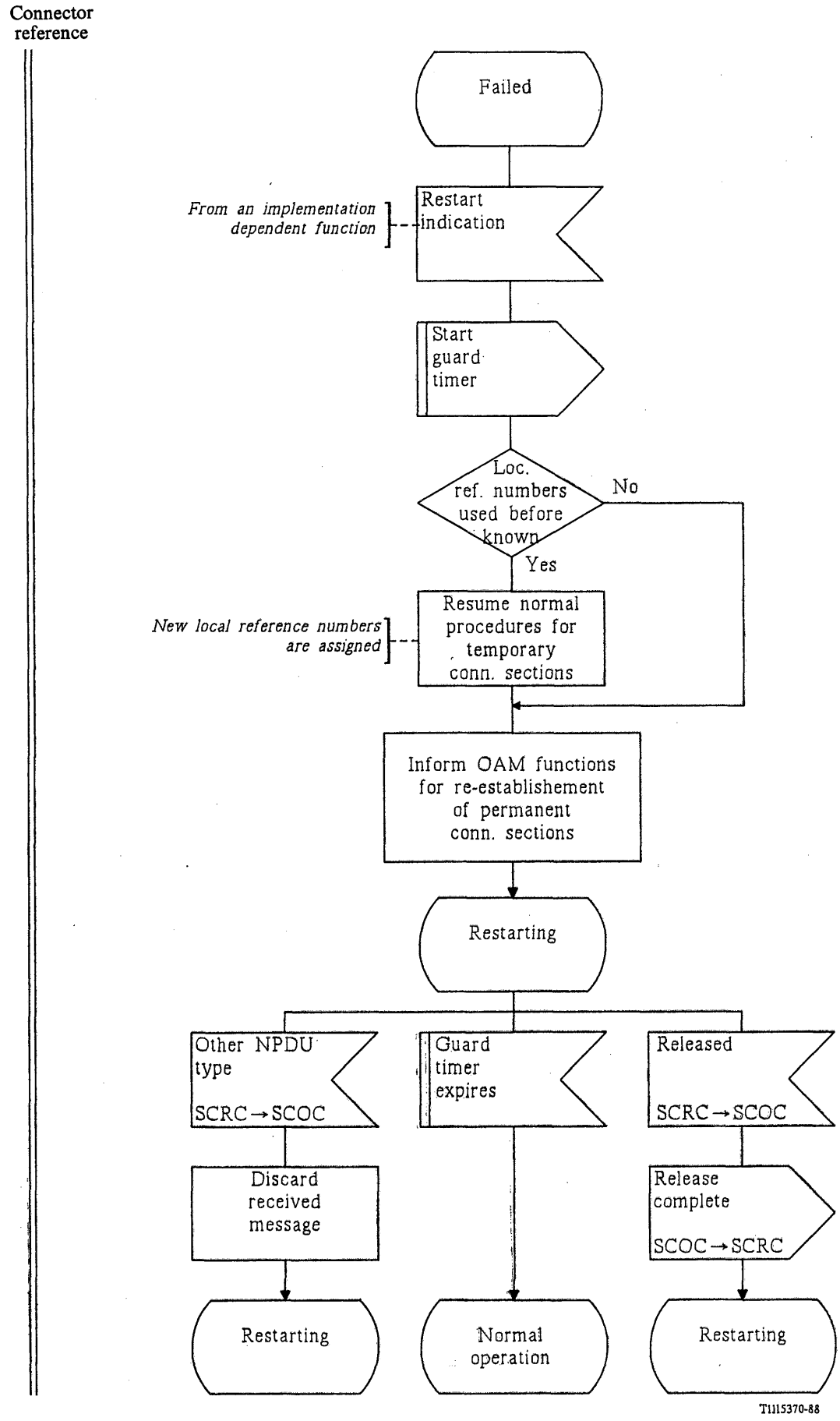



FIGURE C-11/Q.714

**Restart procedure for SCCP connection-oriented control (SCOC)**

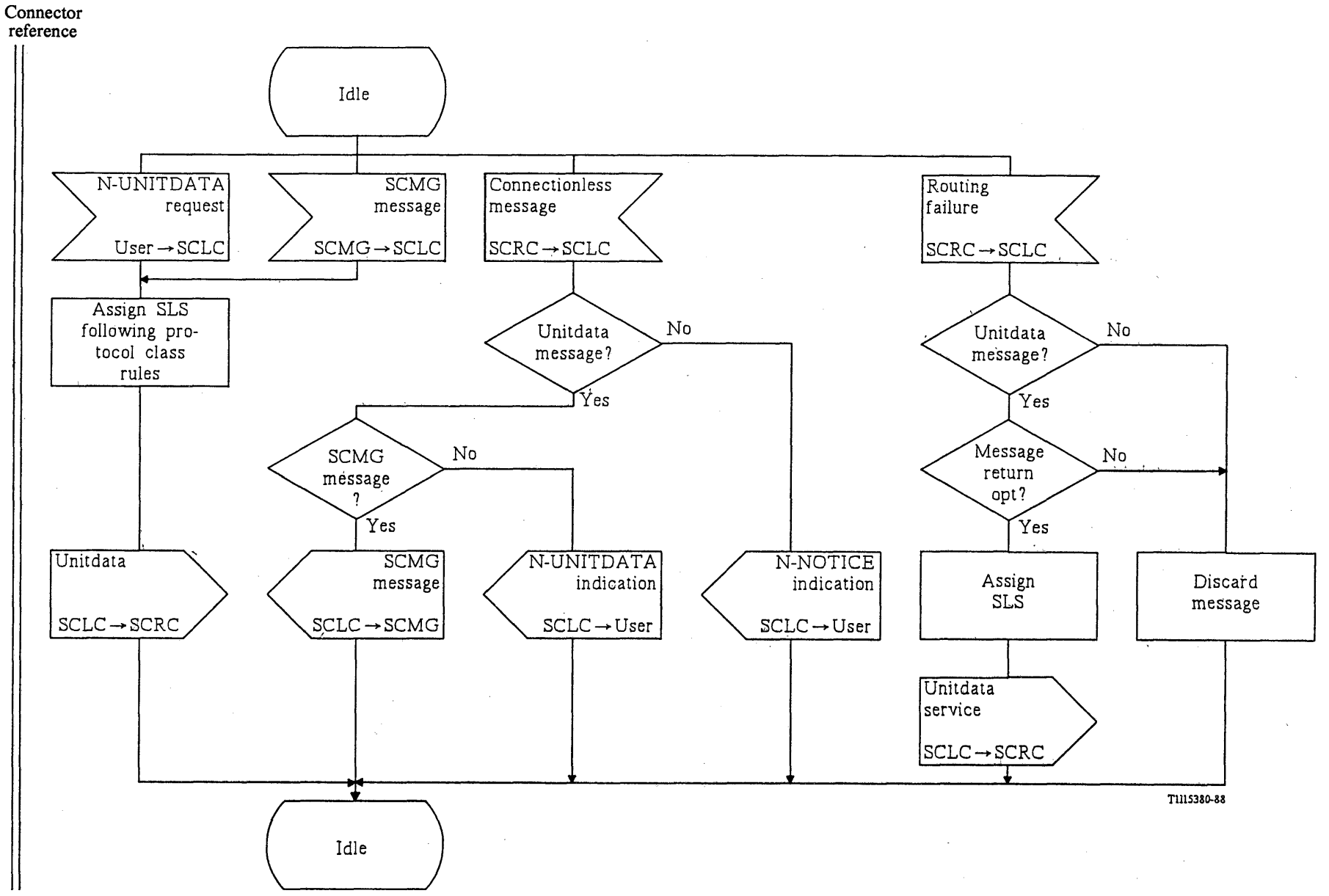



FIGURE C-12/Q.714

**SCCP connectionless control (SCLC)**

ANNEX D

(to Recommendation Q.714)

**State transition diagrams (STD) for SCCP management control**

D.1 *General*

This Annex contains the description of the SCCP management (SCMG) function according to the CCITT Specification and Description Language (SDL).

For the SCCP management function, Figure D-1/Q.714 illustrates a subdivision into functional blocks, showing their functional interactions as well as the functional interactions with the other major functions (e.g. SCCP connectionless control (SCLC)). This is followed by Figures D-2/Q.714 to D-10/Q.714 showing state transition diagrams for each of the functional blocks.

The detailed functional breakdown shown in the following diagrams is intended to illustrate a reference model, and to assist interpretation of the text of the SCCP management procedures. The state transition diagrams are intended to show precisely the behaviour of the signalling system under normal and abnormal conditions as viewed from a remote location. It must be emphasized that the functional partitioning shown in the following diagrams is used only to facilitate understanding of the system behaviour, and is not intended to specify the functional partitioning to be adopted in a practical implementation of the signalling system.

D.2 *Drafting conventions*

Each major function is designated by its acronym (e.g. SCMG = SCCP management).

Each functional block is also designated by an acronym which identifies it (e.g. SSAC = Sub-System Allowed Control).

External inputs and outputs are used for interactions between different functional blocks. Included within each input and output symbol in the state transition diagrams are acronyms which identify the functional blocks which are the source and the destination of the message, e.g.:

SSAC → SSTC indicates that the message is sent from Sub-System Allowed Control to Sub-System Test Control.

Internal inputs and outputs are only used to indicate control of timers.

D.3 *Figures*

Figure D-1/Q.714 shows a subdivision of the SCCP management function (SCMG) into smaller functional blocks, and also shows the functional interactions between them. Each of these functional blocks is described in detail in a state transition diagram as follows:

a) Signalling Point Prohibited Control (SPPC) is shown in Figure D-2/Q.714;
b) Signalling Point Allowed Control (SPAC) is shown in Figure D-3/Q.714;
c) Signalling Point Congested Control (SPCC) is shown in Figure D-4/Q.714;
d) Sub-System Prohibited Control (SSPC) is shown in Figure D-5/Q.714;
e) Sub-System Allowed Control (SSAC) is shown in Figure D-6/Q.714;
f) Sub-System Status Test Control (SSTC) is shown in Figure D-7/Q.714;
g) Coordinated State Change Control (CSCC) is shown in Figure D-8/Q.714;
h) Local Broadcast (LBCS) is shown in Figure D-9/Q.714;
i) Broadcast (BCST) is shown in Figure D-10/Q.714.

D.4 *Abbreviations and timers*

Abbreviations and timers used in Figures D-1/Q.714 to D-10/Q.714 are listed below.

*Abbreviations*

BCST Broadcast
CSCC Cooordinated State Change Control
DPC Destination Point Code
LBCS Local Broadcast
MSG Message
MTP Message Transfer Part
SCCP Signalling Connection Control Part

| | |
|---|---|
| SCLC | SCCP Connectionless Control |
| SCMG | SCCP Management |
| SCOC | SCCP Connection-Oriented Control |
| SCRC | SCCP Routing Control |
| SOG | Sub-System Out of Service Grant |
| SOR | Sub-System Out of Service Request |
| SP | Signalling Point |
| SPAC | Signalling Point Allowed Control |
| SPCC | Signalling Point Congested Control |
| SPPC | Signalling Point Prohibited Control |
| SS | Sub-System |
| SSA | Sub-System Allowed |
| SSAC | Sub-System Allowed Control |
| SSP | Sub-System Prohibited |
| SSPC | Sub-System Prohibited Control |
| SST | Sub-System Status Test |
| SSTC | Sub-System Status Test Control |
| UIS | User In Service |
| UOS | User Out of Service |

*Timers*

| | |
|---|---|
| T(stat. info.) | Delay between requests for sub-system status information |
| T(coord. chg.) | Waiting for grant for sub-system to go out of service |
| T(ignore SST) | Delay for sub-system between receiving grant to go out of service and actually going out of service |

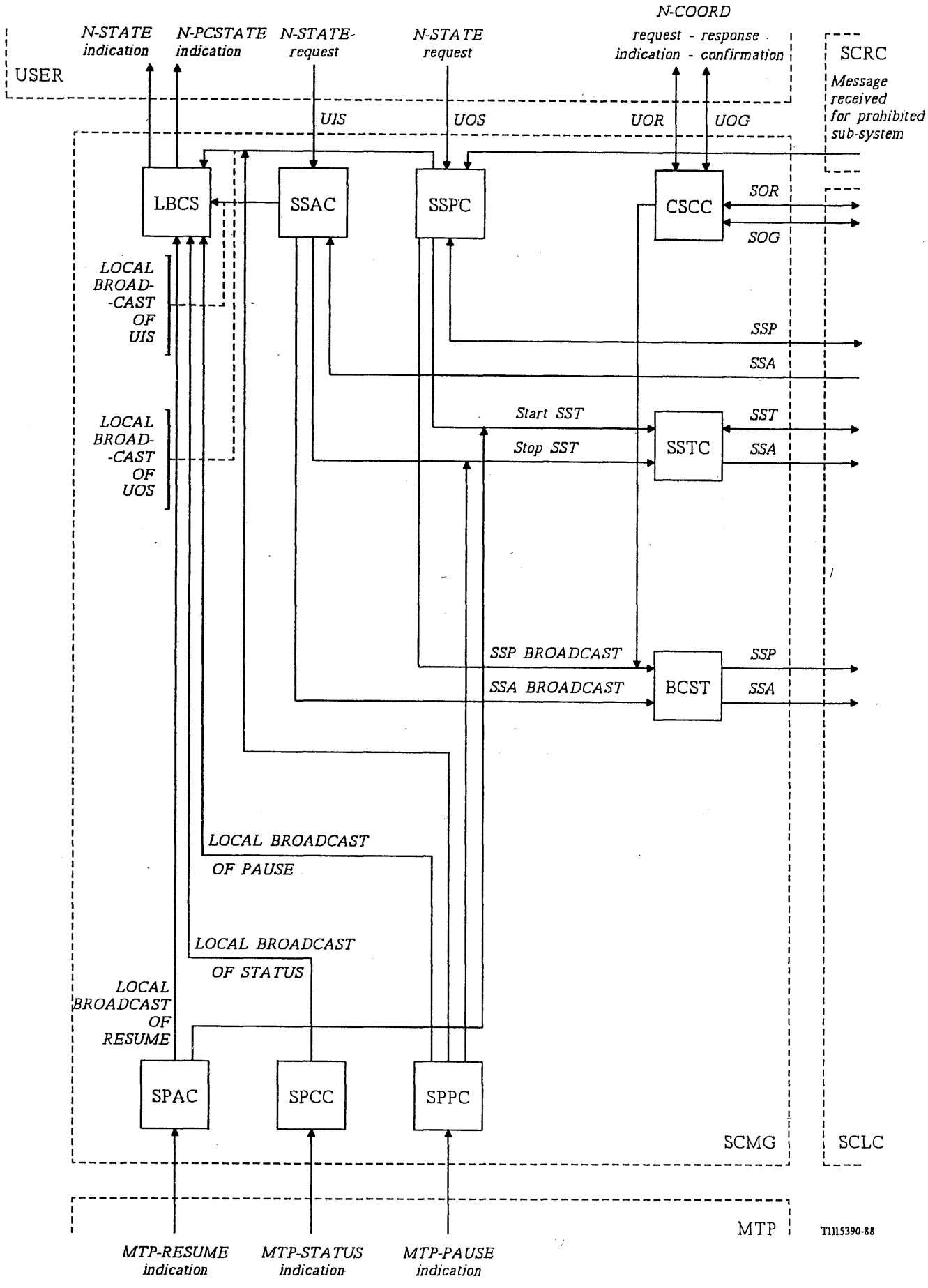



FIGURE D-1/Q.714

**SCCP management overview (SCMG)**

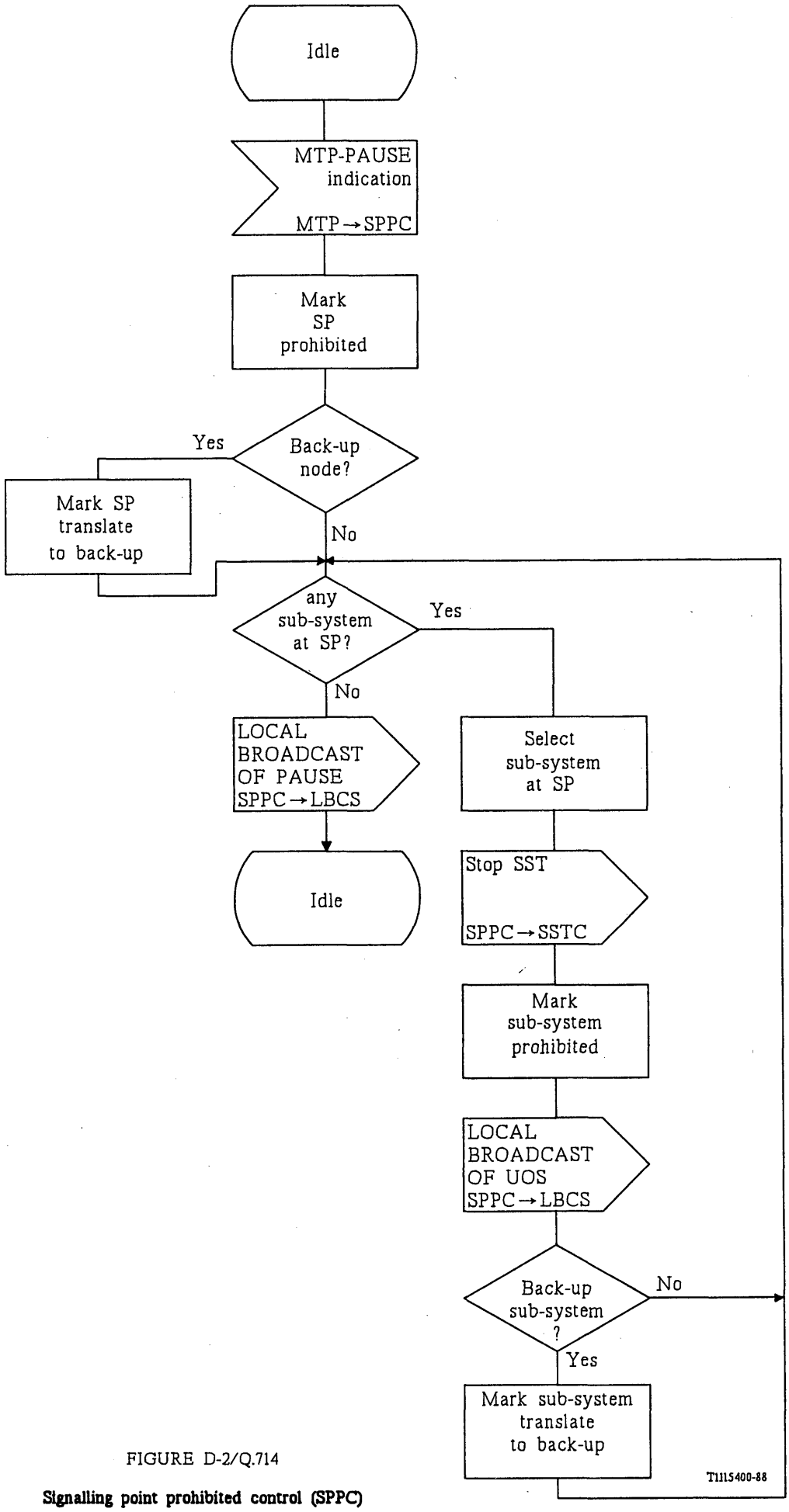



FIGURE D-2/Q.714

**Signalling point prohibited control (SPPC)**

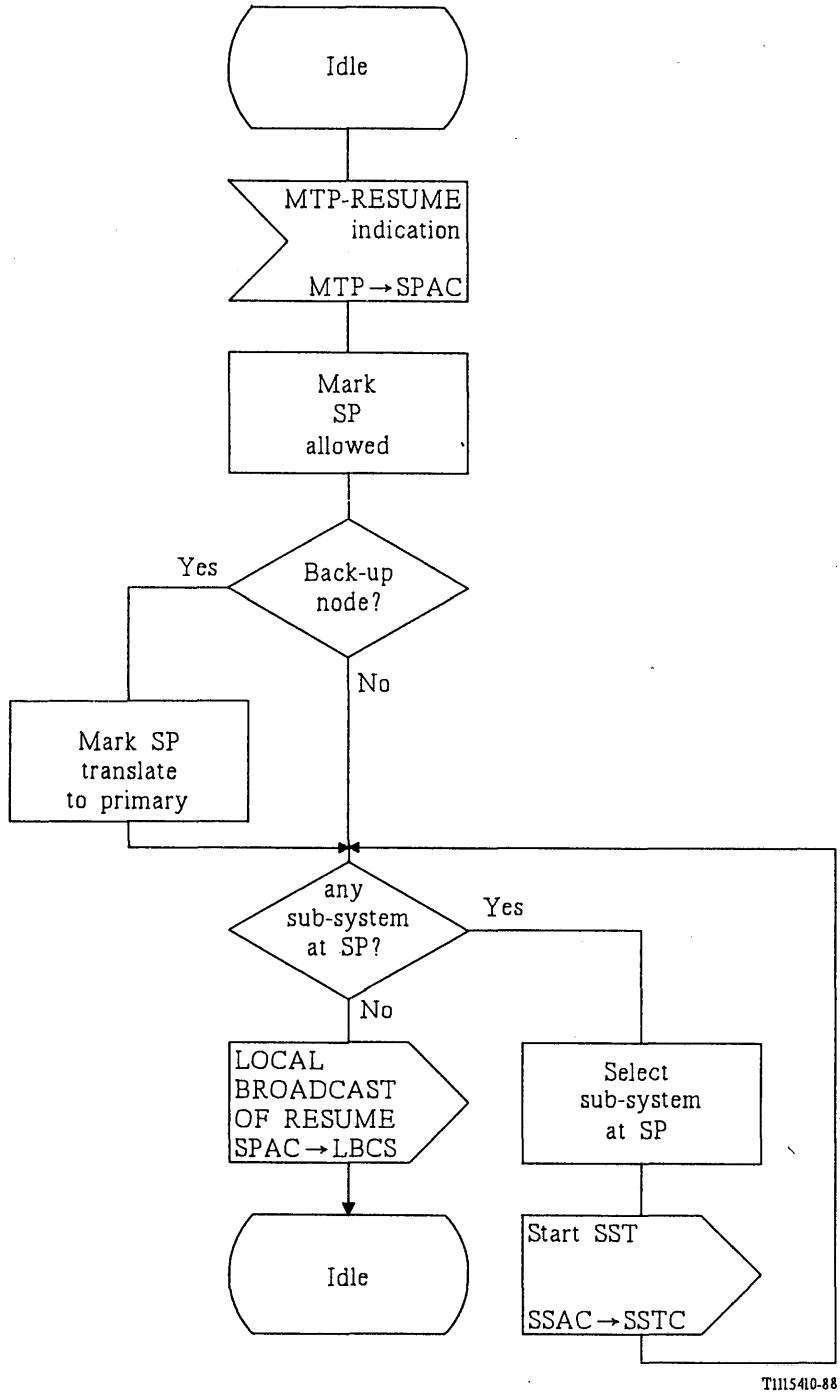



FIGURE D-3/Q.714

**Signalling point allowed control (SPAC)**

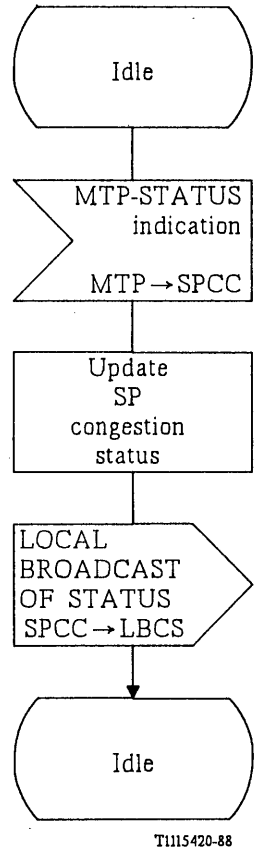



FIGURE D-4/Q.714

**Signalling point congested control (SPCC)**

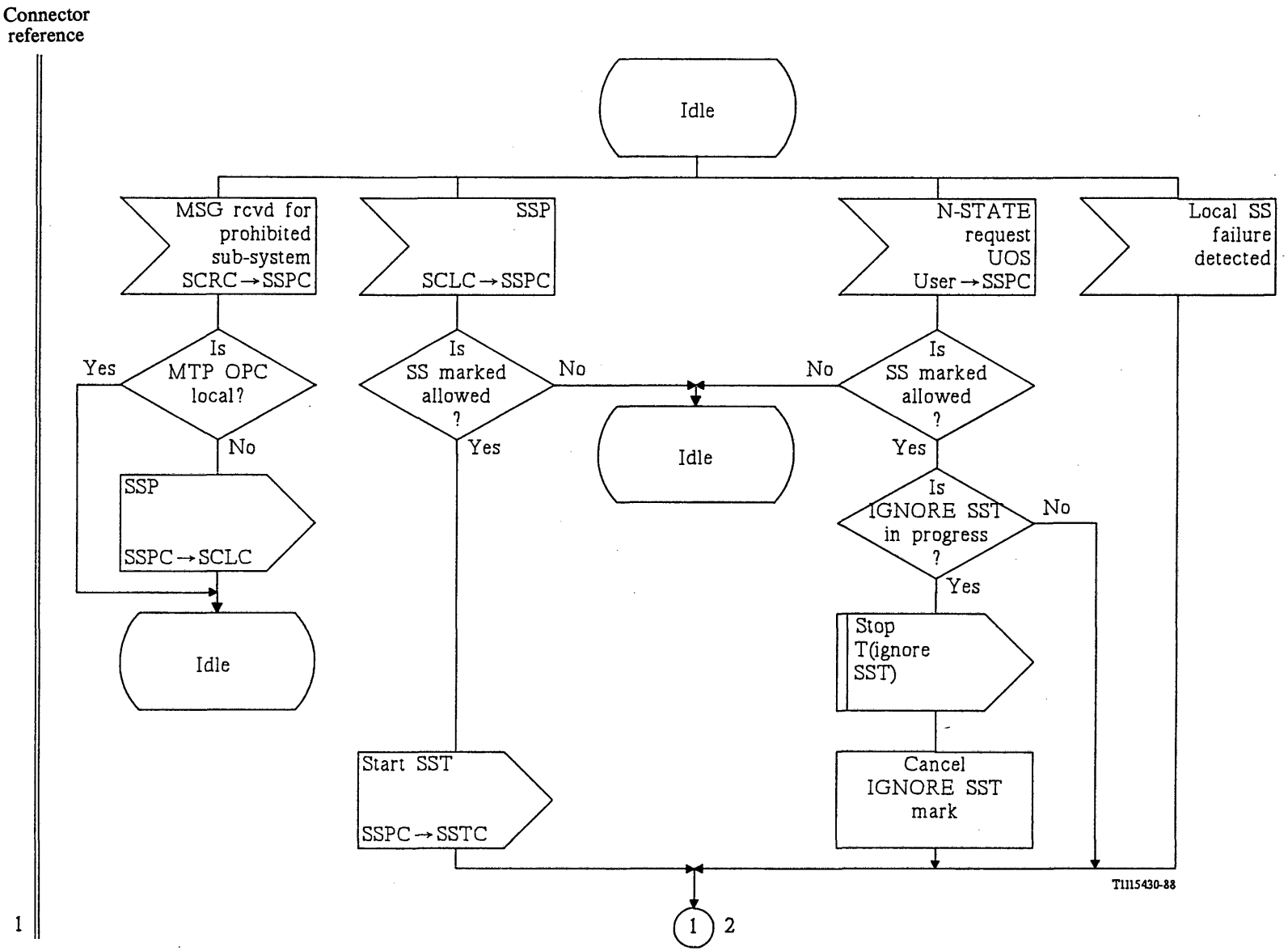



FIGURE D-5/Q.714 (Sheet 1 of 2)

**Sub-system prohibited control (SSPC)**

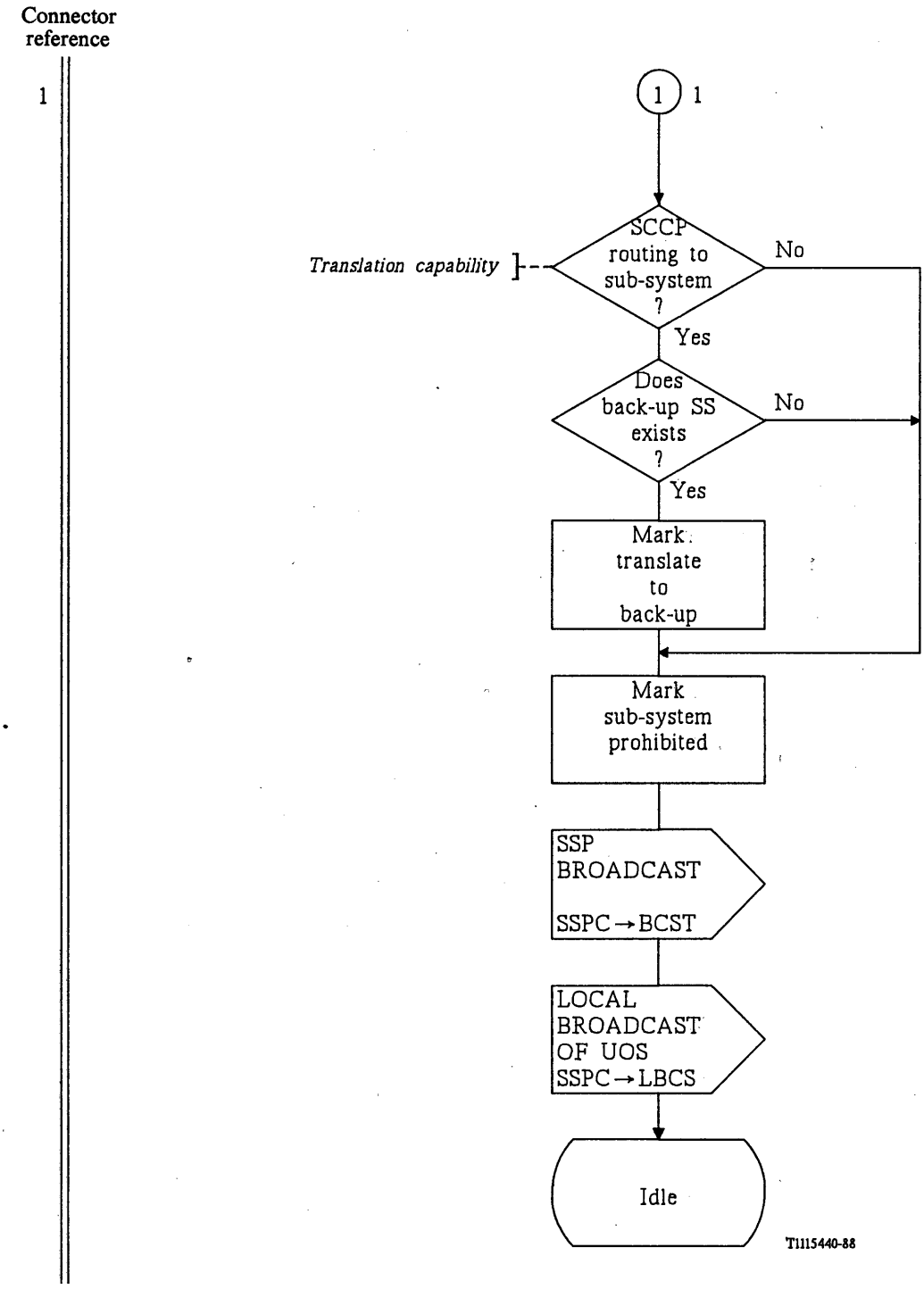



FIGURE D-5/Q.714 (Sheet 2 of 2)

**Sub-system prohibited control (SSPC)**

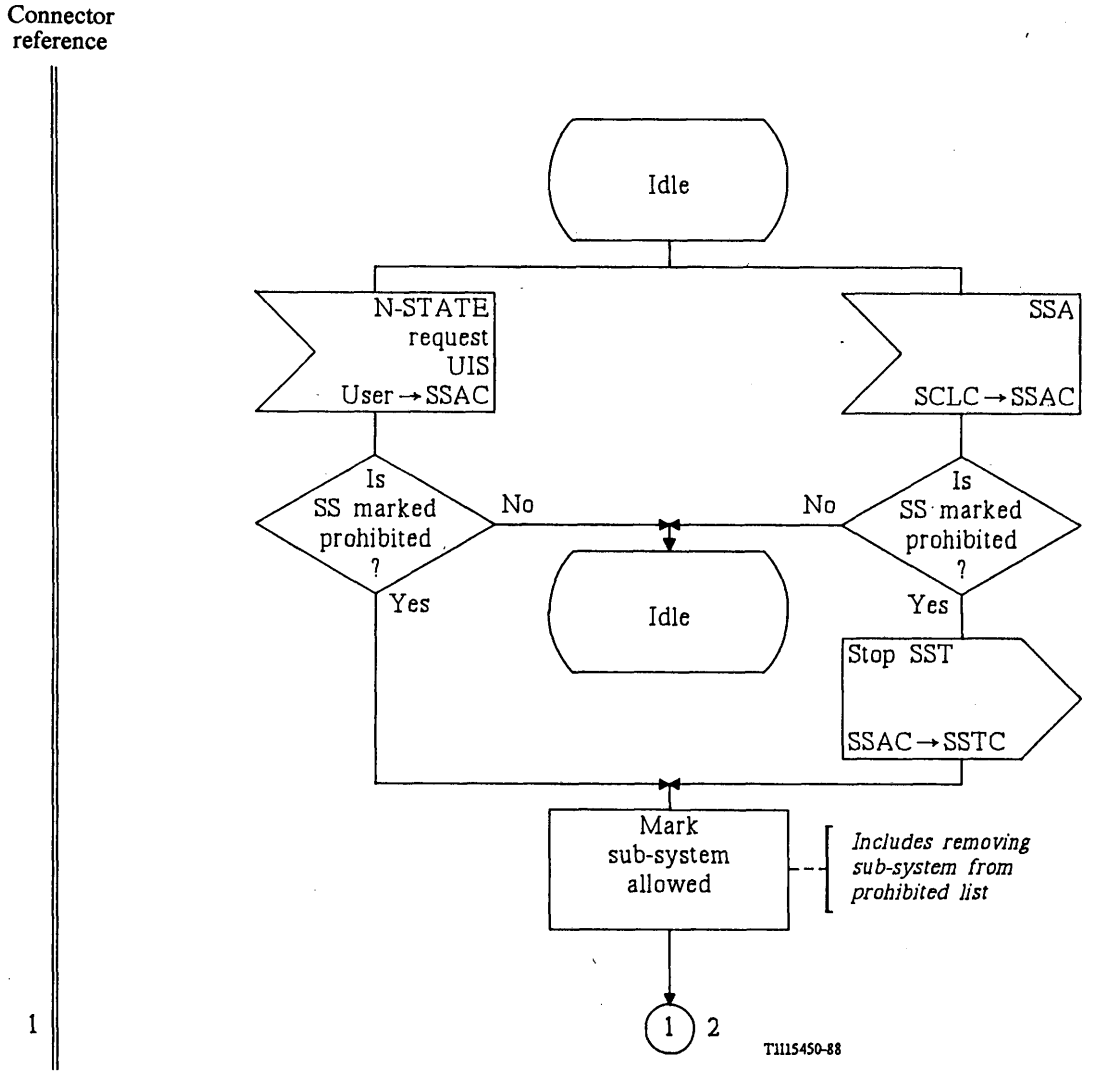



FIGURE D-6/Q.714 (Sheet 1 of 2)

**Sub-system allowed control (SSAC)**

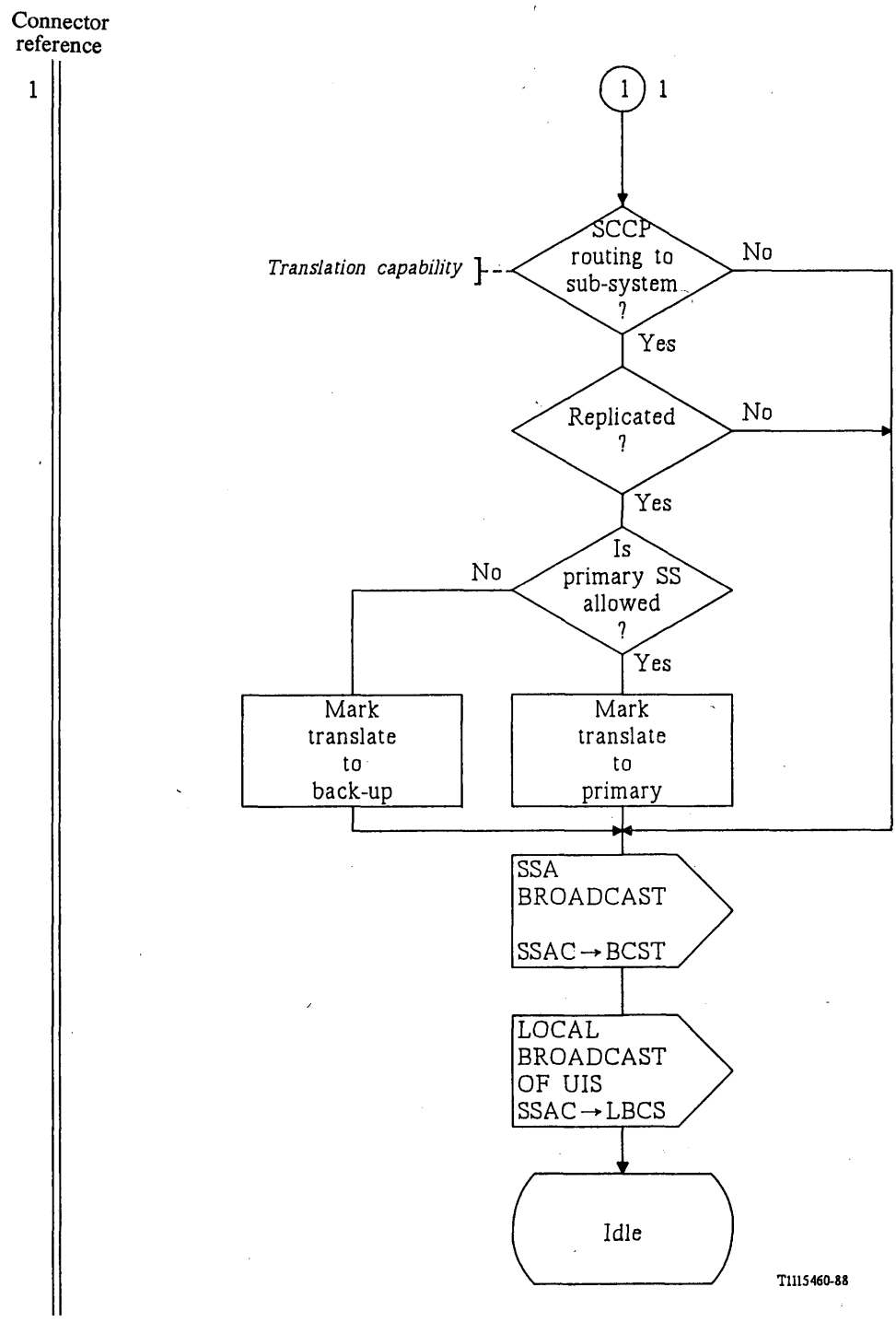



FIGURE D-6/Q.714 (Sheet 2 of 2)

**Sub-system allowed control (SSAC)**

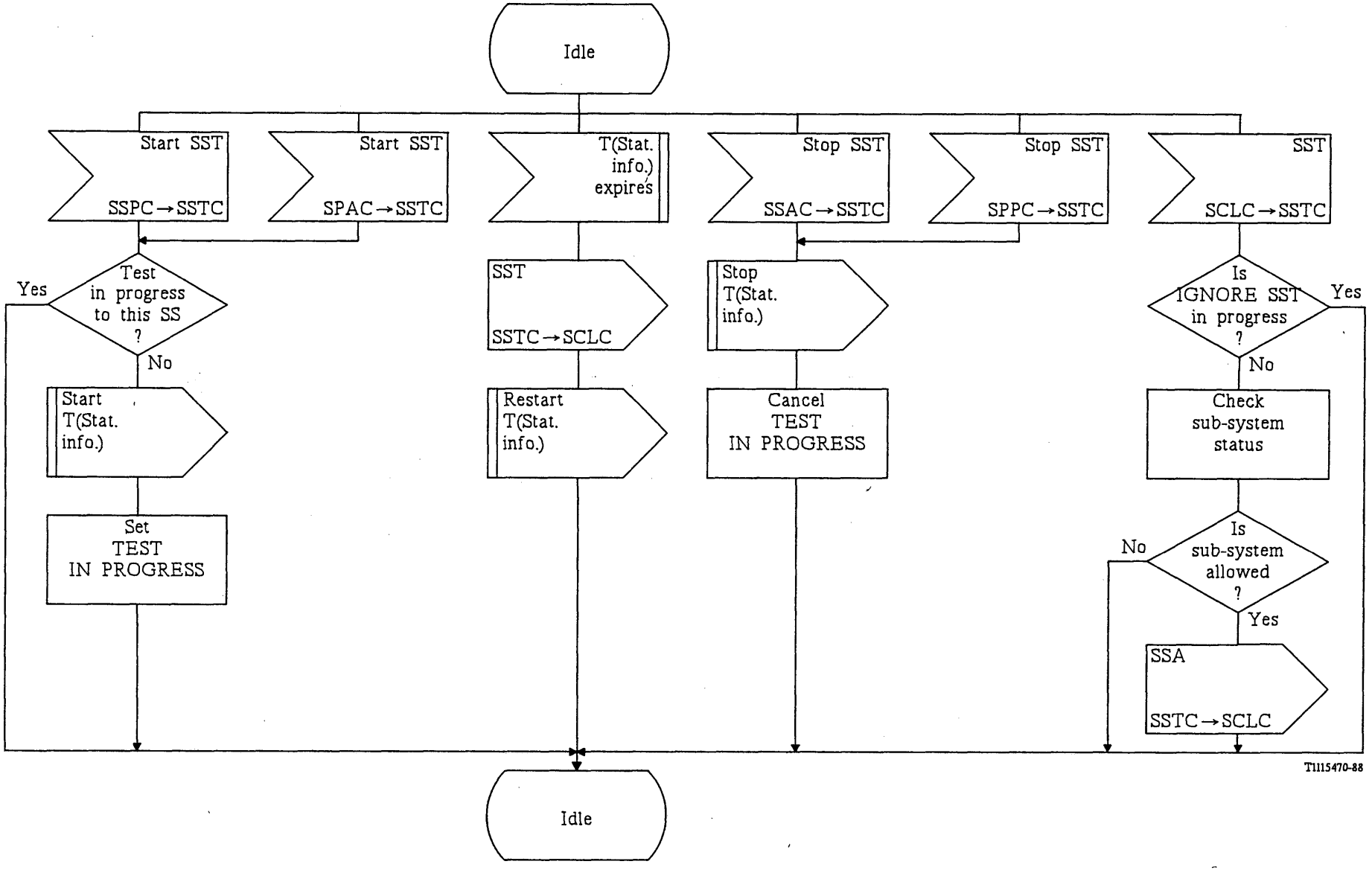



FIGURE D-7/Q.714

**Sub-system Status Test Control (SSTC)**

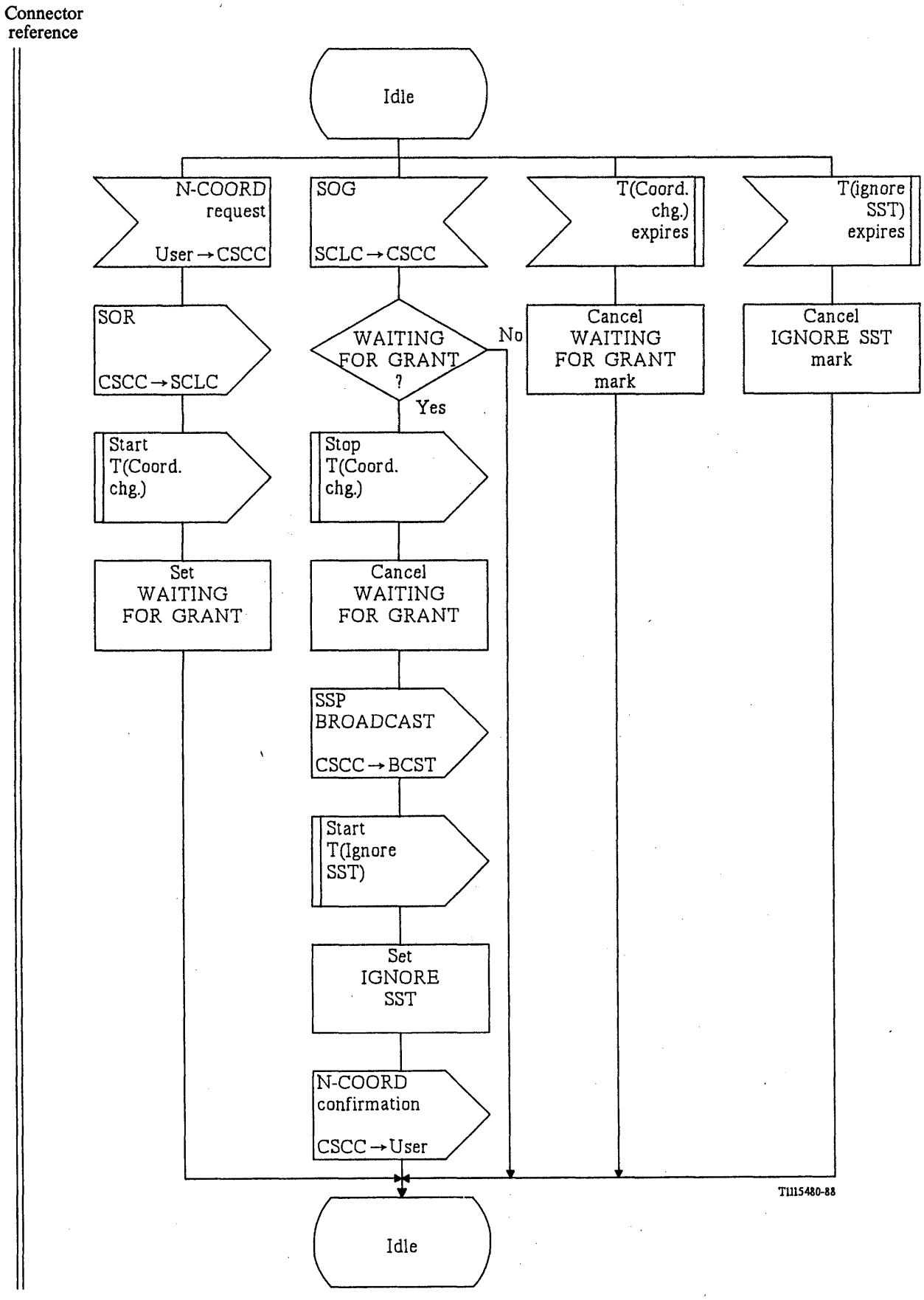



FIGURE D-8/Q.714 (Sheet 1 of 2)

**Coordinated State Change Control (CSCC) at the requesting node**

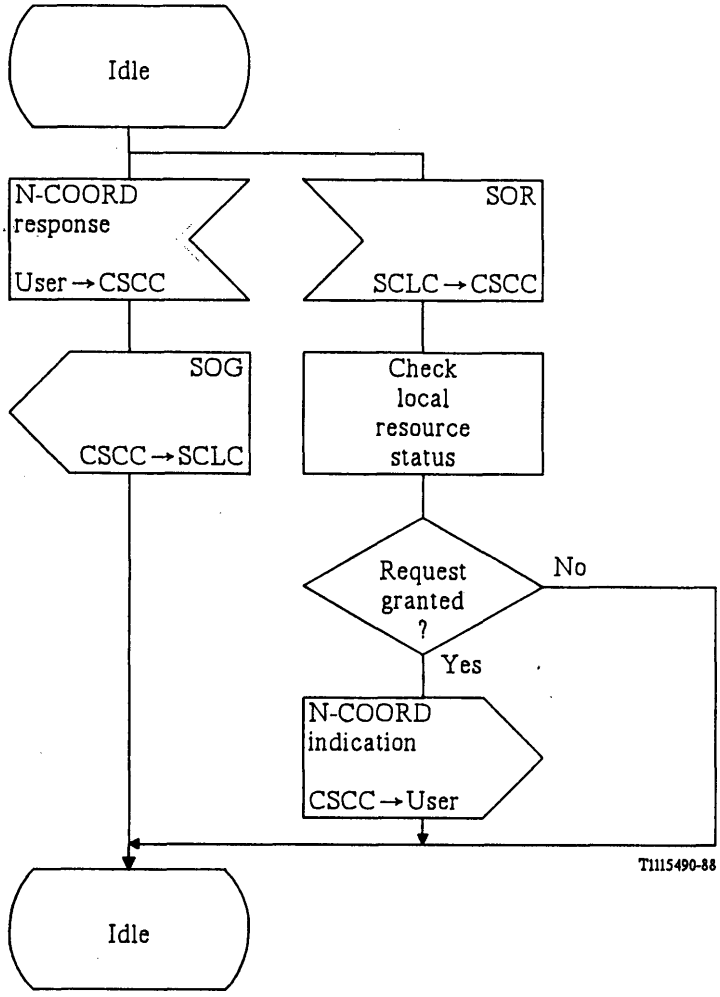
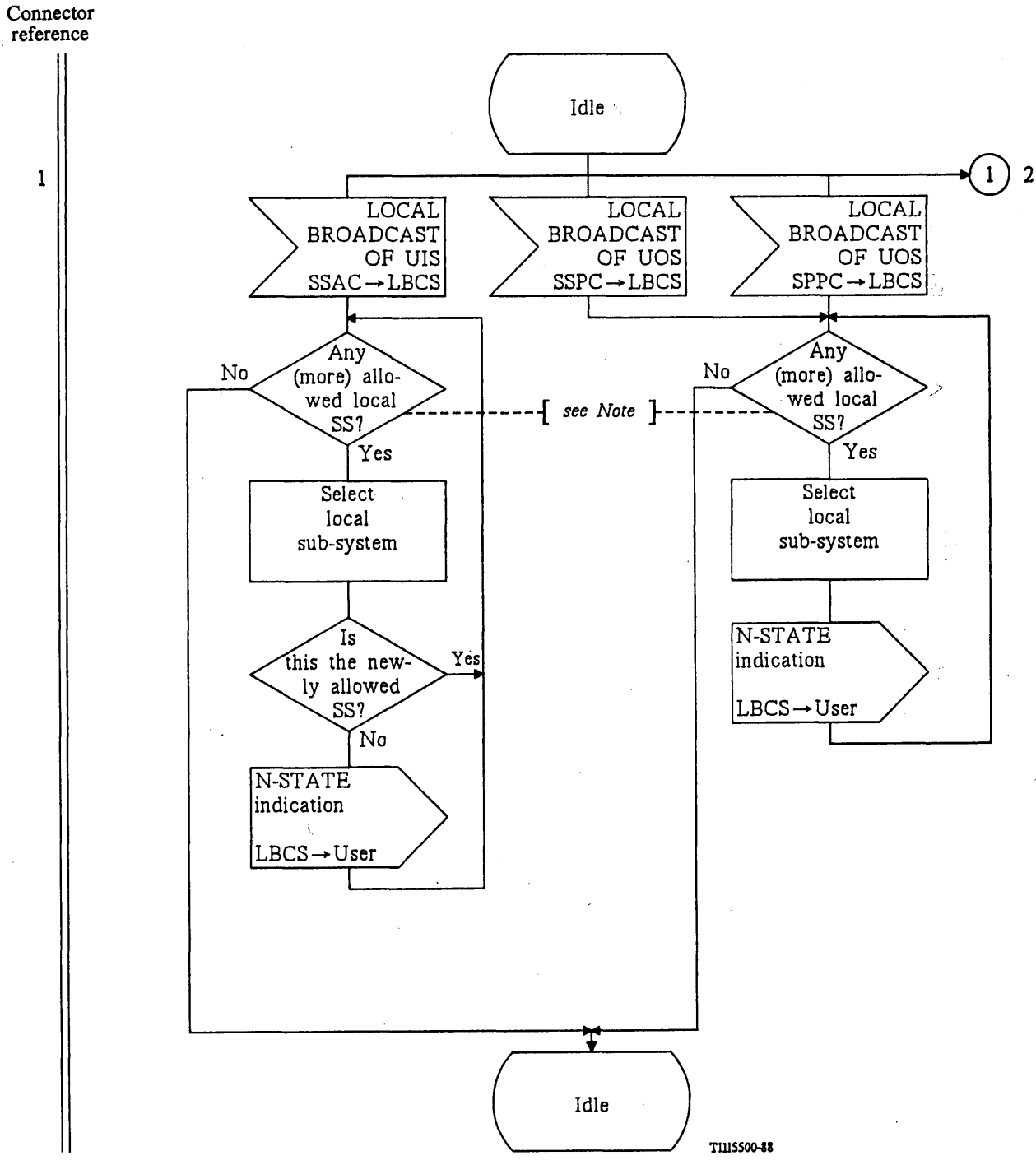



FIGURE D-8/Q.714 (Sheet 2 of 2)

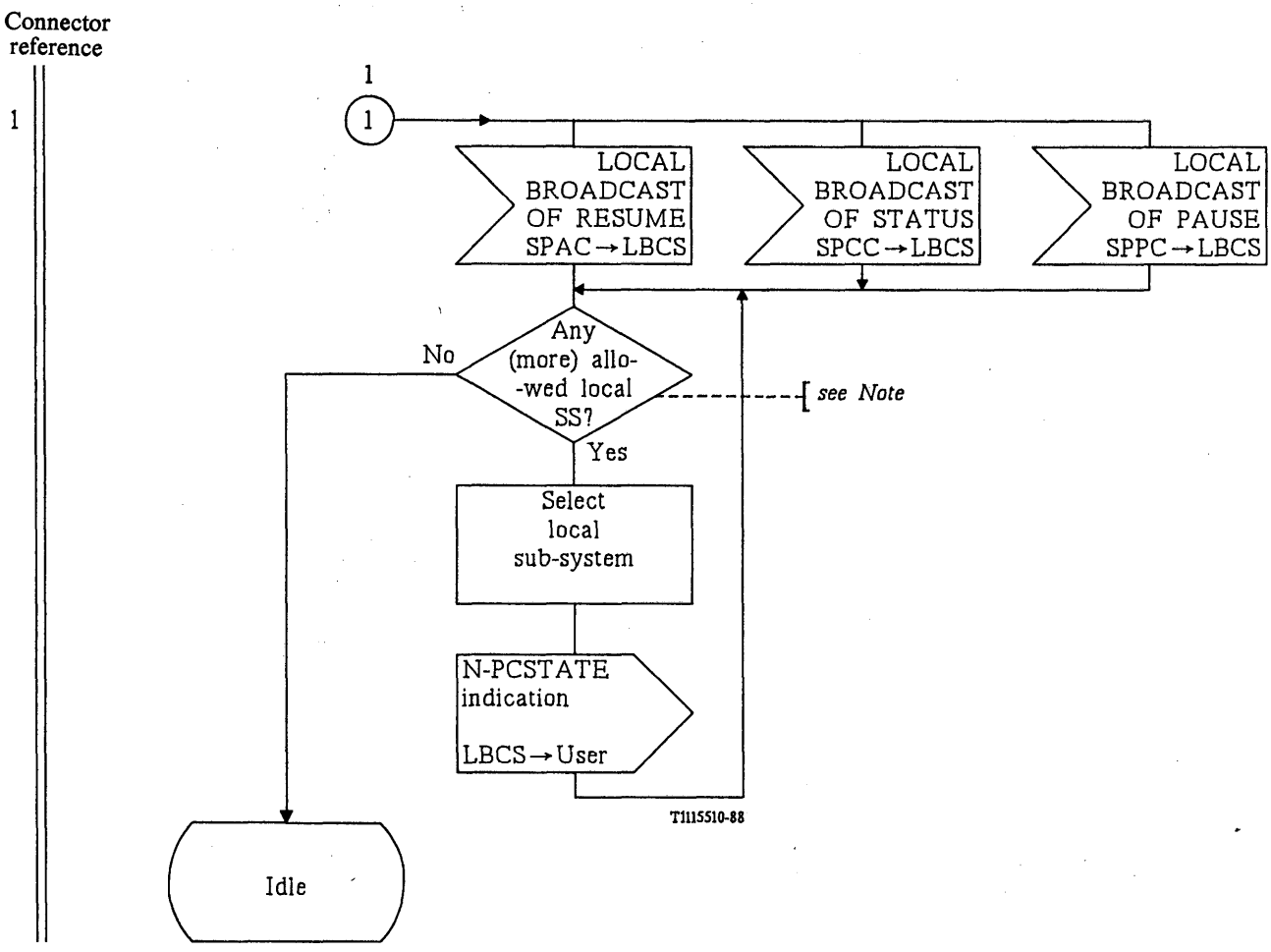
**Coordinated State Change control (CSCC) at the granting node**




*Note* – As specified in § 5.3.6.1 in Recommendation Q.714, only concerned sub-systems are informed.

FIGURE D-9/Q.714 (Sheet 1 of 2)

**Local broadcast (LBCS)**




*Note* – As specified in § 5.3.6.1 in Recommendation Q.714, only concerned sub-systems are informed.

FIGURE D-9/Q.714 (Sheet 2 of 2)

**Local broadcast (LBCS)**

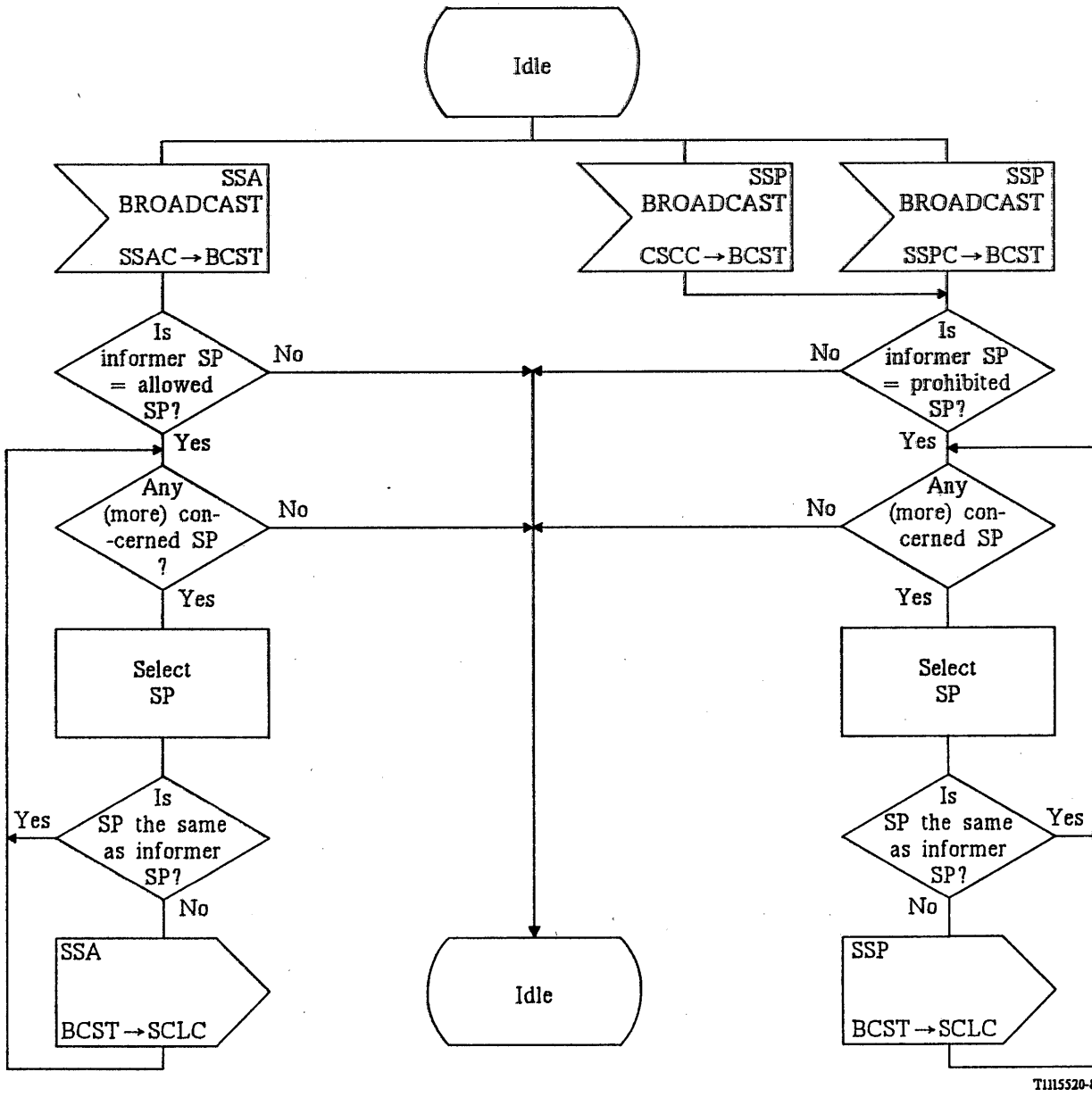



FIGURE D-10/Q.714

**Broadcast (BCST)**

# SIGNALLING CONNECTION CONTROL PART (SCCP) PERFORMANCES

## 1 General

### 1.1 *Overview*

The Signalling Connection Control Part (SCCP) of Signalling System No. 7 is designed as a general message transport system common to the various sub-systems which are using its services.

SCCP must satisfy the requirements of these various sub-systems and therefore the most stringent sub-system requirements are considered when defining a value for a performance parameter (most stringent at the time of the specification). To this end, the requirements of ISDN-UP, the OMAP, the dialogue between an exchange and a Service Control Point (using the Transaction Capabilities), in particular, were investigated. It is assumed that a SCCP which satisfies the requirements of these users mentioned above will also meet those of future users.

SCCP performances are defined by parameters of two kinds:

- quality of service parameters as seen by a user of the SCCP;
- internal parameters which are not seen by the user but which contribute to a quality of service parameter: for example the transfer delay in a relay point which contributes to the total transit delay of messages as seen by the user.

The definitions of all these parameters are presented in Section 2 of this Recommendation. Then the values allowed for the internal parameters are defined in Section 3. Values for the quality of service parameters are given in Recommendation Q.709 which deals with HSRCs.

### 1.2 *Definitions*

Two concepts must be defined when dealig with SCCP performances: SCCP route and SCCP relation. These concepts are similar to the one defined for the MTP (i.e. signalling route and signalling relation). They are defined as follows:

- **SCCP route**: A SCCP route is composed of an ordered list of nodes where the SCCP is used (origin, relay(s), destination) for the transfer of SCCP messages from an originating SCCP user to the destination SCCP user.
- **SCCP relation**: A SCCP relation is a relation between two SCCP users which allows them to exchange data over it. A SCCP relation can consist of one or several SCCP routes.

Five types of nodes where SCCP functions are involved are defined as follows:

- **originating node** (origin of a UDT message or of a signalling connection).
- **destination node** (destination of a UDT message or of a signalling connection).
- **relay point**: signalling point where the translation functions of the SCCP for connectionless classes are implemented.
- **relay point without coupling**: signalling point where the relay functions of the SCCP connection oriented classes, but without the coupling of signalling connection sections function, are implemented.
- **relay point with coupling**: signalling point where the relay functions of the SCCP connection oriented classes, including the coupling of signalling connection sections function, are implemented.

## 2 Definition of performance parameters

Some parameters which are defined in this section cannot be measured from the outside of a signalling point and therefore no values are attributed to them in Section 3 where only measurable values are given. This is true for some internal parameters such as for example the transit time of a CR message for the relay function at a relay point without coupling: this parameter does not include in its definition the time due to the MTP and therefore in Section 3 values are given to the transit time at a relay point which icludes both the time spent in the SCCP and the MTP.

In networks containing implementations from a number of different vendors, it may be necessary where a parameter has a send and receive component to specify that parameter on such a basis. This will then ensure that the overall requirement is satisfied.

### 2.1 *Performance parameters for the connectionless classes*

#### 2.1.1 *Quality of service parameters*

The following parameters define the quality of service as seen by a user of the connectionless classes of the SCCP:

- **undetected errors**

  This parameter gives the probability that a UDT message is delivered with user data which is defective.

- **residual error probability**

  This parameter gives the probability that a UDT message is lost, duplicated or delivered incorrectly by the set constituted of SCCP and the MTP (called Network Service Part or NSP). An incorrectly delivered UDT is one in which the user data are delivered in a corrupted condition (see undetected errors above), or the user data are delivered to an incorrect NSAP.

  For class 1 only, a UDT message is considered as incorrectly delivered if it is delivered out of sequence by the NSP.

- **out of sequence probability**

  This parameter gives the probability that UDT messages are delivered out of sequence to the user by the NSP.

  *Note* – This parameter is relevant only for class 1.

- **total transit delay of a UDT message**

  This parameter is the elapsed time between a N-UNITDATA request issued by a SCCP user at the originating node and the correponding N-UNIDATA indication issued to the SCCP user at the destination node.

  This parameter is composed of several internal parameters:

  - sending time of a UDT message by the SCCP
  - MTP overall transfer time
  - transit time of a UDT message for the relay function at a relay point
  - receiving time of a UDT message by the SCCP

  Depending on the configuration, the second parameter could appear one or several times and the third parameter could appear zero, one or several times. This is illustrated in Figure 1/Q.716.

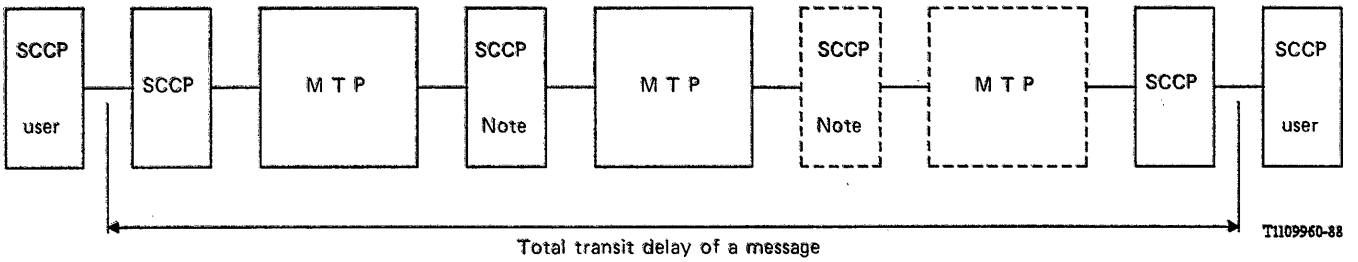
  A probabilistic approach has to be taken to give values to this parameter, considering the various possible SCCP routes and the existence of queues at several points.

- **unavailability of a SCCP relation**

  This parameter characterizes the inability for two SCCP users to communicate via the NSP.

  This parameter is determined by the unavailability of the individual components of a SCCP relation: SCCP at the two endpoints, one or several signalling relations and zero, one or several relay points.

  This unavailability can be reduced by the duplication of routes at the SCCP level.




*Note* – Zero, one or several relay points can be present depending on the network configuration.

FIGURE 1/Q.716

**Functional diagram of the total transit delay of a message**

### 2.1.2 *Internal parameters*

The following parameters are internal to the network service but they contribute to the quality of service as components of a parameter of the previous section for connectionless classes of the SCCP.

– **sending time of a UDT message by the SCCP**

This parameter is the elapsed time between a N-UNIDATA request and the corresponding MTP-TRANSFER request at the originating node.

*Note* – The value of this parameter may differ substantially depending whether or not a translation function is used in the SCCP.

– **MTP overall transfer time**

This parameter is already defined in Recommendation Q.706 as parameter T0 in § 4.3.3.

– **transit time of a UDT message for the relay function at a relay point**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive corresponding to an incoming UDT message at a relay point (i.e. a signalling point where are implemented the SCCP translation functions), and the associated MTP-TRANSFER request primitive corresponding to the outgoing UDT message (which may differ from the incoming one by the called party address).

A probabilistic approach has to be taken to give values to this parameter, considering the existence of queues and that it is possible for the translation functions to be congested.

– **receiving time of a UDT message by the SCCP**

This parameter is the elapsed time between a MTP-TRANSFER indication and the corresponding N-UNIDATA indication at the destination node.

– **unavailability of a relay point**

This parameter characterizes the unavailability of the translation functions of the SCCP at a relay point.

## 2.2 *Performance parameters for the connection oriented classes*

### 2.2.1 *Quality of service parameters*

The following parameters define the quality of service as seen by a user of the connection oriented classes of the SCCP.

- **signalling connection establishment time**

  This parameter is the elapsed time between a N-CONNECT request and the corresponding N-CONNECT confirmation primitive for a successful signalling connection establishment.

  This delay is composed of two parameters: one which depends of the user at the destination node and one which depends of the NSP. The first one which is the elapsed time between a N-CONNECT indication and response at the destination will be specified for each user. The second one is an internal parameter of the SCCP and will be called SCCP component of the signalling connection establishment time. It will be specified in this SCCP performances Recommendation.

  Moreover it is possible to specify here the maximum signalling connection establishment time. It is equal to the connection establishment timer (see Recommendation Q.714).

- **signalling connection establishment failure probability**

  A signalling connection establishment failure is defined as a connection refusal or a time-out for the connection establishment timer coming from the SCCP.

  The dimensioning of the SCCP regarding the number of local reference numbers will impact this signalling connection establishment failure probability. The unavailability of a SCCP relation is also an internal parameter impacting this probability.

  The connection refusals coming from the called user must not be taken into account. This also applies for the time-out coming from this called user.

  *Note* – It is possible for the connection refusals to distinguish between the one coming from the user and the one coming from the SCCP, but that is impossible for the time-out of the connection establishment timer.

- **throughput**

  This parameter is specified independently for each direction of transmission and corresponds to a number of octets of user data (contained in NSDU) transferred per second on a signalling connection.

  *Note* – Only successfully transferred user data are taken into account; that means: to the correct destination, error-free and without missequencing.

- **overall transit time of DT messages**

  This parameter is the elapsed time between a N-DATA request and the corresponding N-DATA indication.

  This parameter is composed of several internal parameters:

  - sending time of a DT message by the SCCP,
  - MTP overall transfer time,
  - transit time of a DT message for the relay function at a relay point with coupling,
  - receiving time of a DT message by the SCCP.

  Depending of the configuration of the signalling connection, the second parameter could appear one or several times and the third parameter could appear zero, one or several times (see Figure 1/Q.716).

  A probabilistic approach has to be taken to give values to this parameter, considering the various possible SCCP routes and the existence of queues at several points.

- **undetected errors**

  This parameter gives the probability that a DT message is delivered with user data which is defective.

- **residual error rate for DT messages**

  This parameter gives the probability that a DT message is lost, duplicated, missequenced or incorrectly delivered by the NSP.

  A DT message is incorrectly delivered if user data is delivered in a corrupted condition (see undetected errors above), or the user data are delivered to an incorrect NSAP.

– **out of sequence probability for DT messages**

This parameter gives the probability that DT messages are delivered out of sequence to the user by the NSP.

– **signalling connection unsolicited reset and premature release probability**

This parameter gives the probability that a connection release or reinitialization due to the SCCP occurs on a signalling connection during a given time.

The unavailability of a SCCP relation is an internal parameter to be considered when calculating the probability of a connection release occurence due to the SCCP.

– **signalling connection reset delay**

This parameter is the elapsed time between a N-RESET request and the corresponding N-RESET confirmation primitive for a successful signalling connection reset.

### 2.2.2 *Internal parameters*

The following parameters are internal to the network service but they contribute to the quality of service as components of a parameter of the previous section for connection oriented classes of the SCCP.

– **SCCP component of the signalling connection establishment time**

This parameter is composed of two times:

- the elapsed time between a N-CONNECT request primitive at the origin node and the corresponding N-CONNECT indication primitive at the destination node.
- the elapsed time between a N-CONNECT response primitive at the destination node and the corresponding N-CONNECT confirmation primitive at the origin node.

It is composed of several internal parameters:

- Sending time of a CR message by the SCCP
- MTP overall transfer time
- Transit time of a CR message for the relay function at a relay point without coupling
- Transit time of a CR message for the relay function at a relay point with coupling
- Receiving time of a CR message by the SCCP
- Sending time of a CC message by the SCCP
- Transit time of a CC message for the relay function at a relay point with coupling
- Receiving time of a CC message by the SCCP

Depending on the configuration these parameters can appear zero, one or several times.

A probabilistic approach has to be taken to give values to this parameter, considering the various possible configurations and the existence of queues at several points.

– **sending time of a CR message by the SCCP**

This parameter is the elapsed time between the N-CONNECT request primitive and the corresponding MTP-TRANSFER request primitive (for the transfer of the CR message).

*Note* – The value of this parameter may differ substantially depending wether or not a translation function is used in the SCCP.

– **MTP overall transfer time**

This parameter is already defined in Recommendation Q.706 as parameter T0 in § 4.3.3.

– **transit time of a CR message for the relay function at a relay point without coupling**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive corresponding to an incoming CR message at a relay point without coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing CR message.

– **transit time of a CR message for the relay function at a relay point with coupling**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive corresponding to an incoming CR message at a relay point with coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing CR message (which may differ from the incoming one only by the called party address).

– **receiving time of a CR message by the SCCP**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive (for an incoming CR message), and the corresponding N-CONNECT indication primitive.

– **sending time of a CC message by the SCCP**

This parameter is the elapsed time between a N-CONNECT respose primitive and the corresponding MTP-TRANSFER request primitive (for the transfer of the CC message).

– **transit time of a CC message for the relay function at a relay point with coupling**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive corresponding to an incoming CC message at a relay point with coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing CR message.

– **receiving time of a CC message by the SCCP**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive (for an incoming CC message), and the corresponding N-CONNECT confirmation primitive.

– **unavailability of a SCCP relation**

This parameter characterizes the inability for two SCCP users to communicate via the NSP.

This parameter is determined by the unavailability of the individual components of a SCCP relation: SCCP at the two endpoints, one or several signalling relations and zero, one or several relay points with coupling and without coupling.

The unavailability can be reduced by the duplication of routes at the SCCP level.

– **unavailability of a relay point**

This parameter characterizes the unavailability of the SCCP at a relay point.

– **sending time of a DT message by the SCCP**

This parameter is the elapsed time between a N-DATA request primitive and the corresponding MTP-TRANSFER request primitive (for the transfer of a DT message).

– **transit time of a DT message for the relay function at a relay point with coupling**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive corresponding to an incoming DT message at a relay point with coupling, and the associated MTP-TRANSFER request primitive corresponding to the outgoing DT message.

– **receiving time of a DT message by the SCCP**

This parameter is the elapsed time between a MTP-TRANSFER indication primitive (for an incoming DT message), and the corresponding N-DATA indication primitive.

### 2.3 *Correspondence between the QOS parameters and the class*

The correspondence between the quality of service parameters defined in §§ 2.1.1 and 2.2.1 above and their applicability to the various classes of the SCCP are illustrated in Table 1/Q.716 below.

## 3 Specified values for internal parameters

### 3.1 *Internal parameters for classes 0 and 1*

*Transit time of a UDT message in a relay point*

The transit time of a UDT message in a relay point is composed of the transit time of a UDT message for the relay function in a relay point and of the time elapsed in the MTP at this relay point for the UDT message: it is measurable externally. It is described in Figure 2/Q.716 and it should not exceed the values given in Table 2/Q.716.

TABLE 1/Q.716

| Parameter | Protocol class | | | |
|---|---|---|---|---|
| | 0 | 1 | 2 | 3 |
| Undetected errors | Y | Y | Y | Y |
| Residual error probability | Y | Y | Y | Y |
| Out of sequence probability | N | Y | Y | Y |
| Total transit delay of a message | Y | Y | Y | Y |
| Unavailability of a SCCP relation | Y | Y | Y | Y |
| Signalling connection establishment time | N | N | Y | Y |
| Signalling connection establishment failure probability | N | N | Y | Y |
| Throughput | N | N | Y | Y |
| Signalling connection unsolicited reset and premature release probability | N | N | Y | Y |
| Signalling connection reset delay | N | N | N | Y |

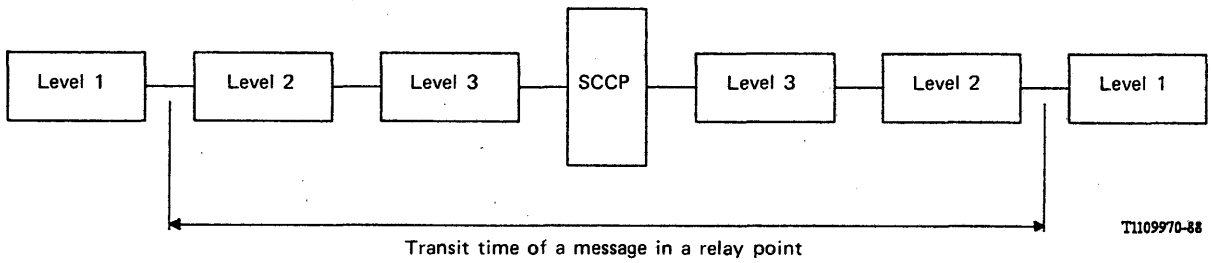



FIGURE 2/Q.716

**Functional diagram for the transit time of a message in a relay point**

TABLE 2/Q.716

| Traffic load for the translation function | Transit time of a UDT message in a relay point (in ms) | |
|---|---|---|
| | Mean | 95% |
| Normal | 50 - 155 | 100 - 310 |
| +15% | 100 - 233 | 200 - 465 |
| +30% | 250 - 388 | 500 - 775 |

*Note* – All values are provisional.

The normal traffic load for the translation function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/Q.706 (short messages with a mean message length of 120 bits). For long messages (272 octets of SIF) it is necessary to add about 30 ms to each figure, to take into account the emitting time at 64 kbit/s much longer for long messages than for short messages.

*Unavailability of a relay point*

The unavailability of a relay point should not exceed $10^{-4}$.

3.2 *Internal parameters for classes 2 and 3*

*Transit time of a CR message at a relay point without coupling*

The transit time of a CR message at a relay point without coupling is composed of the transit time of a CR message for the relay function in a relay point without coupling and of the time elapsed in the MTP at this relay point without coupling for the CR message: it is measurable externally. It should not exceed the values given in Table 3/Q.716.

TABLE 3/Q.716

| Traffic load for the relay function | Transit time of a CR message in a relay point without coupling (in ms) | |
|---|---|---|
| | Mean | 95% |
| Normal | 50 - 155 | 100 - 310 |
| +15% | 100 - 233 | 200 - 465 |
| +30% | 250 - 388 | 500 - 775 |

*Note* – All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/Q.706 (short messages with a mean message length of 120 bits). For long messages (128 octets of SCCP user data) it is necessary to add about 15 ms to each figure, to take into account the emitting time at 64 kbit/s much longer for long messages than for short messages.

*Transit time of a CR message in a relay point with coupling*

The transit time of a CR message at a relay point with coupling is composed of the transit time of a CR message for the relay function in a relay point with coupling and of the time elapsed in the MTP at this relay point with coupling for the CR message: it is measurable externally. It should not exceed the values given in Table 4/Q.716.

TABLE 4/Q.716

| Traffic load for the relay function | Transit time of a CR message in a relay point with coupling (in ms) | |
|---|---|---|
| | Mean | 95% |
| Normal | 75 - 180 | 150 - 360 |
| +15% | 150 - 270 | 300 - 540 |
| +30% | 375 - 450 | 750 - 900 |

*Note* – All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/Q.706 (short messages with a mean message length of 120 bits). For long messages (128 octets of SCCP user data) it is necessary to add about 15 ms to each figure, to take into account the emitting time at 64 kbit/s much longer for long messages than for short messages.

*Transit time of a CC message in a relay point with coupling*

The transit time of a CC message at a relay point with coupling is composed of the transit time of a CC message for the relay function in a relay point with coupling and of the time elapsed in the MTP at this relay point with coupling for the CC message: it is measurable externally. It should not exceed the values given in Table 5/Q.716.

TABLE 5/Q.716

| Traffic load for the relay function | Transit time of a CC message in a relay point with coupling (in ms) | |
|---|---|---|
| | Mean | 95% |
| Normal | 30 - 110 | 60 - 220 |
| +15% | 60 - 165 | 120 - 330 |
| +30% | 150 - 275 | 300 - 550 |

*Note* – All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/Q.706 (short messages with a mean message length of 120 bits). For long messages (128 octets of SCCP user data) it is necessary to add about 15 ms to each figure, to take into account the emitting time at 64 kbit/s much longer for long messages than for short messages.

*Transit time of a DT message in a relay point with coupling*

The transit time of a DT message (DT1 or DT2) at a relay point with coupling is composed of the transit time of a DT message for the relay function in a relay point with coupling and of the time elapsed in the MTP at this relay point with coupling for the DT message: it is measurable externally. It should not exceed the values given in Table 6/Q.716.

TABLE 6/Q.716

| Traffic load for the relay function | Transit time of a DT message in a relay point with coupling (in ms) | |
|---|---|---|
| | Mean | 95% |
| Normal | 30 - 110 | 60 - 220 |
| +15% | 60 - 165 | 120 - 330 |
| +30% | 150 - 275 | 300 - 550 |

*Note* – All values are provisional.

The normal traffic load for the relay function is the load for which the point is dimensioned.

These figures assume a message length distribution as given in Table 2/Q.706 (short messages with a mean message length of 120 bits). For long messages (255 octets of SCCP user data) it is necessary to add about 30 ms to each figure, to take into account the emitting time at 64 kbit/s much longer for long messages than for short messages.

*Unavailability of a relay point without coupling*

The unavailability of a relay point without coupling should not exceed $10^{-4}$.

*Unavailability of a relay point with coupling*

The unavailability of a relay point with coupling is for further study.

## GLOSSARY OF TERMS USED IN SIGNALLING SYSTEM No. 7

**acknowledgement**

*F: accusé de réception*

*S: acuse de recibo*

A service of the SCCP by which the receiver of the message informs the sender of the correct receipt.

**available signalling link**

*F: canal sémaphore disponible*

*S: enlace de señalización disponible*

A signalling link which has successfully completed the initial alignment procedures and carries (or is ready to carry) signalling traffic.

**adjacent signalling points**

*F: points sémaphores adjacents*

*S: puntos de señalización adyacentes*

Two signalling points that are directly interconnected by (a) signalling link(s).

**alignment error rate monitoring**

*F: surveillance du taux d'erreur pendant la procédure d'alignement*

*S: monitor de tasa de errores en la alineación*

A procedure by which the error rate of signalling link is measured during the initial alignment.

**alternative routing (of signalling)**

*F: acheminement (de signalisation) de secours*

*S: encaminamiento alternativo (de señalización)*

The routing of a given signalling traffic flow in case of failures affecting the signalling links, or routes, involved in the normal routing of that signalling traffic flow.

**analogue signalling data link**

*F: liaison sémaphore de données analogique*

*S: enlace analógico de datos de señalización*

The data link that provides an interface to signalling terminals and is made up of voice-frequency analogue transmission channels and modems.

**application**

*F: application*

*S: aplicación*

The set of user's requirements.

**application entity (AE)**

*F: entité d'application (AE)*

*S: entidad de aplicación (EA)*

A set of Application Service Elements which together perform all or part of the communications aspects of an application process. The Application Entity is addressed through an SCCP subsystem number.

**application process**

*F: processus d'application*

*S: proceso de aplicación*

An element which performs the information processing for a particular application.

**application service element (ASE)**

*F: élément de service d'application (ASE)*

*S: elemento del servicio aplicación (ESA)*

A coherent set of integrated functions within an application entity which provides an OSI environment capability, using underlying services where appropriate.

**associated mode (of signalling)**

*F: mode (de signalisation) associé*

*S: modo (de señalización) asociado*

The mode where messages for a signalling relation involving two adjacent signalling points are conveyed over a directly interconnecting signalling link.

**backward indicator bit (BIB)**

*F: bit indicateur vers l'arrière (BIR)*

*S: bit indicador inverso (bit indicador hacia atrás) (BII)*

A bit in a signal unit requesting, by its status change, retransmission at the remote end when a signal unit is received out of sequence.

**backward sequence number (BSN)**

*F: numéro de séquence vers l'arrière (NSR)*

*S: número secuencial inverso (hacia atrás) (NSI)*

A field in a signal unit sent which contains the forward sequence number of a correctly received signal unit being acknowledged.

**basic (error correction) method**

*F: méthode (de correction d'erreur) de base*

*S: método básico (de corrección de errores)*

A non-compelled, positive/negative acknowledgement, retransmission error control system.

**called/calling party address**

*F: adresse du demandé/du demandeur*

*S: dirección de la parte llamada/llamante*

An address within an SCCP message, consisting of any combination of signalling point code, global title and subsystem number.

**changeback**

*F: retour sur canal sémaphore normal*

*S: retorno al enlace de servicio*

The procedure of transferring signalling traffic from one or more alternative signalling links to a signalling link which has become available.

**changeback code**

*F: code de retour sur canal sémaphore normal*

*S: código de retorno al enlace de servicio*

A field in the signalling network management messages used in the changeback procedure; it is used to discriminate messages relating to different changeback procedures performed at the same time towards the same signalling link.

**changeover**

*F: passage sur canal sémaphore de secours*

*S: paso a enlace de reserva*

The procedure of transferring signalling traffic from one signalling link to one or more different signalling links, when the link in use fails or is required to be cleared of traffic.

**check bit (CK)**

*F: bit de contrôle (CRT)*

*S: bit de control (BC)*

A bit associated with a character or block for the purpose of checking the absence of error within the character or block.

**check loop**

*F: boucle pour contrôle de continuité*

*S: bucle de pruebas de continuidad*

A device which is attached to interconnect the Go and Return paths of a circuit at the incoming end of a circuit to permit the outgoing end to make a continuity check on a loop basis.

**circuit identification code (CIC)**

*F: code d'identification de circuit (CIC)*

*S: código de identificación de circuito (CIC)*

Information identifying a circuit between a pair of exchanges, for which signalling is being performed (14 bits in the international ISDN User Part).

**circuit validation test (CVT)**

*F: essai de validation d'un circuit (EVC)*

*S: prueba de validación del circuito (PVC)*

A procedure used to ensure that two exchanges have sufficient and consistent translation data for placing a call on a specific circuit.

**class of operation**

*F: classe d'opération*

*S: clase de operación*

A number indicating whether an operation reports success or failure, failure only, success only or neither.

**class of SCCP service**

*F: classe de service SSCS*

*S: clase de servicio PCCS*

A number chosen by the user of the SCCP to select 1 out of 4 network services provided by the SCCP.

**combined link set**

*F: faisceau combiné de canaux sémaphores*

*S: conjunto combinado de enlaces*

A load sharing collection of one or more link sets.

**common channel signalling**

*F: signalisation par canal sémaphore*

*S: señalización por canal común*

A signalling technique in which signalling information relating to a multiplicity of circuits, and other information such as that used for network management, is conveyed over a single channel by addressed messages.

**component**

*F: composant*

*S: componente*

A protocol data unit exchanged between TC-users, via the Component sublayer of Transaction Capabilities.

**component correlation**

*F: corrélation de composants*

*S: correlación de componentes*

The association of operation invocations and replies.

**component portion**

*F: partie composante*

*S: porción componente*

The part of a TC message containing the Components.

**connection end-point**

*F: point terminal de connexion*

*S: punto extremo de conexión*

A signalling point which may be either originating or destination.

**connection identification**

*F: identification de connexion*

*S: identificación de conexión*

A number which identifies unambiguously a certain connection at the interface between the SCCP and a user function.

**connection-oriented network service**

*F: service de réseau en mode connexion*

*S: servicio de red con conexión*

A network service that establishes logical connections between end users before transferring information.

**connection section**

*F: section de connexion*

*S: sección de conexión*

A section of an SCCP connection between endpoints or between an endpoint and an intermediate point or between intermediate points.

**connectionless network service**

*F: service de réseau en mode sans connexion*

*S: servicio de red sin conexión*

A network service that transfers information between end users without establishing a logical connection or virtual circuits.

**continuity check**

*F: contrôle de continuité*

*S: prueba (verificación) de continuidad*

A check made to a circuit or circuits in a connection to verify that an acceptable path (for transmission of data, speech, etc.) exists.

**continuity check transponder**

*F: répondeur pour contrôle de continuité*

*S: transpondedor (transmisor-respondedor) para pruebas de continuidad*

A device which is used to interconnect the Go and Return paths of a circuit at the incoming end which on detection of a check tone, returns another check tone to the originating end to permit a continuity checking of a 2-wire circuit.

**controlled rerouting**

*F: retour sous contrôle sur route normale*

*S: reencaminamiento controlado*

A procedure of transferring in a controlled way, signalling traffic from an alternative signalling route to the normal signalling route, when this has become available.

**coupling**

*F: couplage*

*S: acoplamiento*

An SCCP function which provides an association between connection sections at a relay point.

**cross-office (transit) delay**

*F: temps (de transit) dans le commutateur*

*S: retardo (de tránsito) a través de la central*

The time a message will take to pass through an exchange.

**cross-office check**

*F: contrôle de continuité à travers un commutateur*

*S: prueba (verificación) de continuidad a través de una central*

A check made of a circuit across the exchange to verify that a transmission path exists.

**data channel propagation time ($T_p$)**

*F: temps de propagation sur la voie de données ($T_p$)*

*S: tiempo de propagación del canal de datos ($T_p$)*

The period which starts when the last bit of the signal unit has entered the data channel at the sending side and ends when the last bit of the signal unit leaves the data channel at the receiving end, irrespective of whether the signal unit is disturbed or not.

**Data User Part (DUP)**

*F: Sous-Système Utilisateur Données (SSUD)*

*S: parte de usuario de datos (PUD)*

The User Part specified for data services.

**destination point (signalling-)**

*F: point (sémaphore) de destination*

*S: punto de destino (de la señalización)*

The signalling point to which a message is destined.

**destination point code (DPC)**

*F: code du point de destination (CPD)*

*S: código del punto de destino (CPD)*

A part of the label in a signalling message which uniquely identifies, in a signalling network, the (signalling) destination point of the message.

**dialogue**

*F: dialogue*

*S: diálogo*

An association established between two TC users exchanging components.

**digital signalling data link**

*F: liaison sémaphore de données numérique*

*S: enlace de datos de señalización digital*

The data link that provides an interface to signalling terminals and is made up of digital transmission channels and digital switches or their terminating equipment.

**dual seizure**

*F: prise simultanée*

*S: doble toma (toma simultánea)*

The condition which occurs when in bothway operation two exchanges attempt to seize the same circuit at approximately the same time.

**emergency changeover**

*F: passage d'urgence sur canal sémaphore de secours*

*S: paso de emergencia a enlace de reserva*

A modified changeover procedure to be used whenever the normal one cannot be accomplished, i.e. in case of some failures in the signalling terminal equipment or in case of inaccessibility between the two involved signalling points.

**end-to-end signalling**

*F: signalisation de bout en bout*

*S: señalización de extremo a extremo*

The capability to transfer signalling information of end point significance directly between signalling end points in order to provide a requesting user with a basic or supplementary service.

**end-user (SCCP)**

*F: utilisateur terminal (SSCS)*

*S: usuario de extremo (PCCS)*

A functional entity above the SCCP upper layer boundary indirectly using the services of the SCCP.

**entity or (N) entity**

*F: entité ou entité (N)*

*S: entidad o entidad (N)*

A set of functions invoked by a given layer for an instance of intersystems communications in which that system is involved. An entity may be partitioned into several sub-entities. For each instance of intersystems communications, the set of functions invoked will be a part of all the functional capability of the given system within the layer in accordance with the functionality required for that instance of inter-system communication.

**expedited data**

*F: données exprés*

*S: datos acelerados (datos expeditados)*

Data transferred with priority which bypasses the normal data flow control.

**failure response time**

*F: temps de réponse à une défaillance*

*S: tiempo de respuesta a fallo*

The elapsed time from the instant a signalling point recognises that a signalling link is unavailable, until the instant when the signalling point completes sending a changeover (or emergency changeover) order to the remote signalling point.

**fill-in signal unit (FISU)**

*F: trame sémaphore de remplissage (TSR)*

*S: unidad de señalización de relleno (USR)*

A signal unit containing only error control and delimitation information, which is transmitted when there are no message signal units or link status signal units to be transmitted.

**flag (F)**

*F: fanion (F)*

*S: bandera (BAN)*

The unique pattern on the signalling data link used to delimit a signal unit.

**flow control**

*F: contrôle de flux*

*S: control de flujo*

A function in a protocol used to control the flow of signalling messages between adjacent layers of a protocol, and/or between peer entities. The function permits, for example, a receiving entity to control signalling message flow from the sending entity.

**forced rerouting**

*F: passage sous contrainte sur route de secours*

*S: reencaminamiento forzado*

A procedure of transferring signalling traffic from one signalling route to another, when the signalling route in use fails or is required to be cleared of traffic.

**forced retransmission (procedure)**

*F: retransmission forcée (procédure de)*

*S: retransmisión forzada (procedimiento de)*

An error correction procedure used to complement the preventive cyclic retransmission procedure.

**forward indicator bit (FIB)**

*F: bit indicateur vers l'avant (BIA)*

*S: bit indicador directo (bit indicador hacia adelante) (BID)*

A bit in a signal unit which indicates the start of a retransmission cycle.

**forward sequence number (FSN)**

*F: numéro de séquence vers l'avant (NSA)*

*S: número secuencial directo (hacia adelante) (NSD)*

A signal unit used to identify the transmitted message signal units.

**function**

*F: fonction*

*S: función*

A logical object which accepts one or more inputs (arguments) and produces a single output (value) uniquely determined by the combination of the input and the formal specification of the function.

**global title (GT)**

*F: appellation globale (AG)*

*S: título global (TG)*

An address used by the SCCP, such as customer dialled digits which does not explicitly contain information that would allow routing in the signalling network, i.e., the SCCP translation function is required.

**hypothetical signalling reference connection (HSRC)**

*F: communication fictive de référence pour la signalisation*

*S: conexión ficticia (o hipotética) de referencia para la señalización (CFRS)*

A hypothetical reference model of a connection in a signalling network.

**identifier (ID)**

*F: identificateur (ID)*

*S: identificador (ID)*

A character, or group of characters, used to identify or name an item of data and possibly to indicate certain properties of that data.

**unavailable signalling link**

*F: canal sémaphore indisponible*

*S: enlace de señalización indisponible*

A signalling link which has been deactivated and cannot therefore carry signalling traffic.

**information element**

*F: élement d'information*

*S: elemento de información*

The basic unit of a TCAP message.

**initial alignment (procedure)**

*F: alignement initial (procédure d')*

*S: alineación inicial (procedimiento de)*

A procedure by which a signalling link becomes able to carry signalling traffic either for the first time or after a failure has occurred.

**integrated digital network (IDN)**

*F: réseau numérique intégré (RNI)*

*S: red digital integrada (RDI)*

A network in which connections established by digital switching are used for the transmission of digital signals.

**integrated services digital network (ISDN)**

*F: réseau numérique avec intégration des services (RNIS)*

*S: red digital de servicios integrados (RDSI)*

An integrated digital network in which the same digital switches and digital paths are used to establish connections for different services, for example, telephony, data.

**Intermediate Service Part**

*F: Sous-Système Services Intermédiaires (SSSI)*

*S: parte servicio intermedio*

An element of Transaction Capabilities which supports TCAP for connection-oriented messages. It represents OSI layers 4 to 6.

**international signalling network**

*F: réseau sémaphore international*

*S: red de señalización internacional*

A network used for signalling, consisting of international signalling points and common channel signalling links connecting them.

**international signalling point**

*F: point sémaphore international*

*S: punto de señalización internacional*

A signalling point which belongs to the international signalling network.

**international signalling point code**

*F: code de point sémaphore international*

*S: código de punto de señalización internacional*

A part of the label in a signalling message that uniquely identifies each signalling point which belongs to the international signalling network. It consists of a sub-field for the signalling area/network code (11-bit) and a sub-field which identifies a signalling point in a specific area or network (3-bit).

**interruption control**

*F: contrôle d'interruption*

*S: protección contra las interrupciones*

A system which monitors a pilot for interruptions on FDM systems and which transmits an indication to the switching equipment.

**ISDN user part (ISDN-UP)**

*F: Sous-Système Utilisateur pour le RNIS (SSUR)*

*S: parte usuario de RDSI (PU-RDSI)*

A protocol of Signalling System No. 7 which provides the signalling functions necessary to basic bearer services and supplementary services for voice and non-voice applications in the ISDN.

**label**

*F: étiquette*

*S: etiqueta*

Information within a signalling message used to identify typically the particular circuit, call or management transaction to which the message is related.

**layer**

*F: couche*

*S: capa*

A group of one or more entities contained within an upper and lower logical boundary. Layer ($N$) has boundaries to the layer ($N + 1$) and to the layer ($N - 1$).

**layer interface**

*F: interface entre couches*

*S: interfaz de capa*

The boundary between two adjacent layers of the model.

**layer service**

*F: service de couche*

*S: servicio de capa*

A capability of the ($N$) layer and the layers beneath it, which is provided to ($N + 1$) entities, at the boundary between the ($N$) layer and the ($N + 1$) layer.

**layer service elements**

*F: elément de service de couche*

*S: elemento de servicio de capa*

An indivisible component of the layer service made visible to the service user via layer primitives.

**layer service primitives**

*F: primitives du service de couche*

*S: primitivas de servicio de capa*

A means for specifying in detail the adjacent layer interactions.

**length indicator (LI)**

*F: indicateur de longueur (INL)*

*S: indicador de longitud (IL)*

A six-bit field which differentiates between message signal units, link status signal units and fill-in signal units and in the case that its binary value is less than 63 indicates the length of a signal unit.

**link-by-link signalling**

*F: signalisation section par section*

*S: señalización enlace por enlace*

A procedure for the exchange of signalling information directly between two signalling points that are either directly connected or via signalling transfer points.

**link state control (LSC)**

*F: supervision de l'état du canal sémaphore (SET)*

*S: control del estado del enlace (CEE)*

Coordinates functions of the signalling link including signal unit delimitation, signal unit alignment, error detection, error correction, initial alignment, signalling link error monitoring and flow control.

**link status signal unit (LSSU)**

*F: trame sémaphore d'état du canal sémaphore (TSE)*

*S: unidad de señalización del estado del enlace (UEE)*

A signal unit which contains status information about the signalling link in which it is transmitted.

**linked operation**

*F: opération liée*

*S: operación enlazada (vinculada)*

An operation invoked from one end of a dialogue that is linked to another operation previously invoked by the other end.

**load sharing (general)**

*F: partage de la charge (en général)*

*S: compartición de carga (en sentido general)*

A process by which signalling traffic is distributed over two or more signalling or message routes, to provide for traffic equalization or security.

**local reference**

*F: référence locale*

*S: referencia local*

A local number, unambiguously identifying an SCCP connection within one SCCP entity.

**management inhibiting**

*F: inhibition par la gestion*

*S: inhabilitación (o inhibición) (en gestión de tráfico de señalización)*

A procedure included in signalling traffic management used to keep a signalling link unavailable to User Part generated signalling traffic, except for test and maintenance traffic.

**mandatory fixed part**

*F: partie obligatoire de longueur fixe*

*S: parte obligatoria fija*

Part of a message that contains those parameters that are mandatory and of fixed length.

**mandatory variable part**

*F: partie obligatoire de longueur variable*

*S: parte obligatoria variable*

Part of a message that contains mandatory parameters of variable length.

**message discrimination**

*F: discrimination des messages (de signalisation)*

*S: discriminación de mensajes*

The process which decides, for each incoming message, whether the signalling point is a destination point or if it should act as a signalling transfer point for that message and accordingly, whether the message should be handed to (signalling) message distribution or to (signalling) message routing functions.

**message distribution**

*F: distribution des messages (de signalisation)*

*S: distribución de mensajes*

The process of determining, upon receipt of a signalling message at its destination point, to which User Part the signalling message is to be delivered.

**message route (signalling-)**

*F: route de message (de signalisation)*

*S: ruta de mensaje (de señalización)*

The signalling link or consecutive links connected in tandem that are used to convey a signalling message from an originating point to its destination point.

**message routing (signalling-)**

*F: acheminement des messages (de signalisation)*

*S: encaminamiento de mensajes (de señalización)*

The process for selecting, for each signalling message to be sent, the signalling link to be used.

**message signal unit (MSU)**

*F: trame sémaphore de message (TSM)*

*S: unidad de señalización de mensaje (USM)*

A signal unit containing a service information octet and a signalling information field which is retransmitted by the signalling link control if it is received in error.

**Message Transfer Part (MTP)**

*F: Sous-Système Transport de Messages (SSTM)*

*S: parte transferencia de mensajes (PTM)*

The functional part of a common channel signalling system which transfers signalling messages as required by all the users, and which performs the necessary subsidiary functions, for example error control and signalling security (levels 1, 2 and 3 of Signalling System No. 7).

**message transfer part receiving time ($T_{mr}$)**

*F: temps de réception du Sous-Système Transport de Messages ($T_{mr}$)*

*S: tiempo de recepción de la parte de transferencia de mensajes ($T_{mr}$)*

The period which starts when the last bit of the signal unit leaves the signalling data link and ends when the last bit of the message has entered the User Part. It includes the handling time at level 2, the transfer time from level 2 to level 3, the handling time at level 3, the transfer time from level 3 to level 4.

**message transfer part sending time ($T_{ms}$)**

*F: temps d'émission du Sous-Système Transport de Messages ($T_{ms}$)*

*S: tiempo de emisión de la parte de transferencia de mensajes ($T_{ms}$)*

The period which starts when the last bit of the message has left the User Part and ends when the last bit of the signal unit enters the data link for the first time. It includes the queueing delay in the absence of disturbances, the transfer time from level 4 to level 3, the handling time at level 3, the transfer time from level 3 to level 2, and handling time in level 2.

**message transfer time at signalling transfer points ($T_{cs}$)**

*F: temps de transfert des messages aux points de transfert sémaphores ($T_{cs}$)*

*S: tiempo de transferencia de mensajes en los puntos de transferencia de señalización ($T_{cs}$)*

The period which starts when the last bit of the signal unit leaves the incoming signalling data link and ends when the last bit of the signal unit enters the outgoing signalling data link for the first time. It includes the queueing delay in the absence of disturbances, but not the additional queueing delay caused by retransmission.

**Mobile Application Part (MAP)**

*F: Sous-Système Application Mobile (SSAM)*

*S: parte aplicación móvil (PAM)*

The Application Entity dedicated to the communication aspects of the mobile application.

**MTP routing verification test (MRVT)**

*F: essai pour la vérification de l'acheminement dans le SSTM (EATP)*

*S: prueba de verificación de encaminamiento por la PTM (PVEM)*

A procedure used to determine if the data of the MTP routing tables in the signalling network are consistent.

**national signalling network**

*F: réseau sémaphore national*

*S: red de señalización nacional*

A network used for signalling, consisting of national signalling points and the connecting common channel signalling links, including the national signalling point of the gateway exchange connected to the internacional signalling network.

**national signalling point (NSP)**

*F: point sémaphore national (PSN)*

*S: punto de señalización nacional (PSN)*

A signalling point which belongs to the national signalling network.

**negative acknowledgement (NACK)**

*F: accusé de réception négatif (ACN)*

*S: acuse de recibo negativo (RN)*

An explicit request for retransmission of signal units, received in a corrupt form.

**network indicator**

*F: indicateur de réseau*

*S: indicador de red*

The part of the subservice field within the service information octet that may be used to discriminate between national and internacional signalling messages.

**Network Service Part (NSP)**

*F: Sous-Système Service Reséau (SSSR)*

*S: parte servicio de red (PSR)*

The combination of the Message Transfer Part and the Signalling Connection Control Part.

**nonassociated mode (of signalling)**

*F: mode (de signalisation) non associé*

*S: modo (de señalización) no asociado*

The mode where messages for a signalling relation involving two (nonadjacent) signalling points are conveyed, between those signalling points, over two or more signalling links in tandem passing through one or more signalling transfer points.

**nonadjacent signalling points**

*F: points sémaphores non adjacents*

*S: puntos de señalización no adyacentes*

Two signalling points that are not directly connected by any signalling links.

**normal routing of (signalling)**

*F: acheminement normal (de signalisation)*

*S: encaminamiento normal (de señalización)*

The routing of a given signalling traffic flow in normal conditions (i.e. in the absence of failures).

**NSAP address (OSI-) (NSAP)**

*F: adresse NSAP (OSI-)*

*S: dirección PASR (ISA-) (PASR)*

A global address as defined for OSI which is understandable over any network and can be used to address between networks.

**operation (TC-)**

*F: opération (GT)*

*S: operación (CT)*

The action being requested of the remote end.

**Operation, Maintenance and Administration Part (OMAP)**

*F: Sous-Système pour l'Exploitation, la Maintenance et la gestion (SSEM)*

*S: parte, operaciones, mantenimiento y administración (POMA)*

The Application Entity dedicated to the communications aspects of the Operation, Administration and Maintenance of the Signalling System No. 7 network and which may have an application for the Telecommunications Management Network (TMN).

**optional part**

*F: partie facultative*

*S: parte opcional (facultativa)*

Part of a message that contains parameters that may or may not occur in any particular message type.

**originating point (signalling-)**

*F: point (sémaphore) d'origine*

*S: punto de origen (de señalización)*

The signalling point in which a message is generated.

**originating point code (OPC)**

*F: code du point d'origine (CPO)*

*S: código del punto de origen (CPO)*

A part of the label in a signalling message which uniquely identifies, in a signalling network, the (signalling) originating point of the message.

**peer entities**

*F: entités homologues*

*S: entidades pares*

Entities in the same layer but in different systems (nodes) which must exchange information to achieve a common objective.

**peer protocol**

*F: protocole homologue*

*S: protocolo para entidades pares*

A formal language used by peer entities to exchange information.

**pilot**

*F: onde pilote*

*S: piloto*

Sinusoidal signal transmitted over analogue FDM links for regulation and supervision purposes.

**pointer**

*F: pointeur*

*S: puntero*

A single octet indicating the beginning of each mandatory variable parameter and optional part.

**positive acknowledgement**

*F: accusé de réception positif*

*S: acuse de recibo positivo*

A way to indicate correct transfer of message signal units.

**preventive cyclic retransmission (error control) method**

*F: méthode (de correction d'erreur) avec retransmission cyclique préventive*

*S: método (de protección contra errores) por retransmisión cíclica preventiva*

A noncompelled, positive acknowledgement, cyclic retransmission forward error correction system.

**processor outage**

*F: processeur hors service*

*S: interrupción del procesador*

A situation in which a signalling link becomes unavailable, due to factors at a functional level higher than level 2. This may be because of, for example, a central processor failure.

**Public Land Mobile Network (PLMN)**

*F: réseau mobile terrestre publique (RMTP)*

*S: red móvil terrestre pública (RMTP)*

A public network dedicated to the operation of mobile radio communications.

**quasi-associated mode (of signalling)**

*F: mode (de signalisation) quasi associé*

*S: modo (de señalización) cuasiasociado*

A nonassociated mode (of signalling) in which the (signalling) message route is determined basically, for each signalling message, by information contained in this message (namely in its routing label) and is fixed in normal operation.

**reply**

*F: réponse*

*S: respuesta*

Any component sent back as the consequence of an operation invocation.

**reset (SCCP)**

*F: reinitialisation (SSCS)*

*S: reinicialización (PCCS)*

A service of the SCCP to return a connection to a predefined state, or to recover from loss of synchronization between two SCCP users.

**restart (SCCP)**

*F: redémarrage (SCCS)*

*S: rearranque (PCCS)*

A recovery mechanism for signalling connection sections in the event of a node failure.

**result**

*F: résultat*

*S: resultado*

The component indicating the outcome (success or failure) of an operation.

**retransmission buffer (RTB)**

*F: tampon de retransmission (TRT)*

*S: memoria tampón de retransmisión (MTR)*

Storage in the signalling link control for signal units transmitted but not yet positively acknowledged.

**retrieval**

*F: récupération*

*S: recuperación*

The process of transferring all those messages in the retransmission buffer of a signalling link (A), which have not yet been positively acknowledged, to the transmission buffers of alternative signalling links.

**route set congestion control**

*F: contrôle d'encombrement de faisceau de routes sémaphores*

*S: control de la congestión de un conjunto de rutas*

A procedure included in the signalling route management which is used to update the congestion status of a signalling route in a given signalling point.

**routing label**

*F: étiquette d'acheminement*

*S: etiqueta de encaminamiento*

The part of the message label that is used for message routing in the signalling network. It includes the destination point code, the originating point code and the signalling link selection field.

**SCCP relation**

*F: relation de SSCS*

*S: relación PCCS*

A relationship between two SCCP users which allows them to exchange data over it. An SCCP relation can consist of one or several routes.

**SCCP relay function**

*F: fonction relais du SSCS*

*S: función de relevo PCCS*

A function which provides an address translation to route an SCCP message to its destination, and may include coupling of connection sections for connection-oriented protocol classes.

**SCCP route**

*F: route du SSCS*

*S: ruta PCCS*

A route composed of an ordered list of nodes where the SCCP is used (origin, relay(s), destination) for the transfer of SCCP messages from an originating SCCP user to the destination SCCP user.

**SCCP routing**

*F: acheminement dans le SSCS*

*S: encaminamiento (por la) PCCS*

A function based on the called party address information, which evaluates and translates the information, checks the addressee availability, and the need for coupling of connection sections.

**SCCP routing verification test (SRVT)**

*F: essai pour la vérification de l'acheminement dans le SSCS (EACP)*

*S: prueba de verificación del encaminamiento PCCS (PVES)*

A procedure used to determine if the data of the SCCP routing tables in the signalling network are consistent.

**SCCP user**

*F: utilisateur du SSCS*

*S: usuario PCCS*

Functional entity which uses directly the services of the SCCP.

**segmenting/reassembling**

*F: segmentation/réassemblage*

*S: segmentación/reensamblado*

If the size of the user data is too big to be transferred within one message, user data are segmented into a number of portions, and reassembled at the receiving end.

**sequence numbering**

*F: numérotation des trames sémaphores*

*S: numeración secuencial*

Each signal unit carries two sequence numbers for error correcting purpose.

**sequencing**

*F: mise en séquence*

*S: secuenciación*

A service of the SCCP that preserves the sequence of Network Service Data Units.

**service indicator (SI)**

*F: indicateur de service (utilisateur) (INS)*

*S: indicador de servicio (IS)*

Information within a signalling message identifying the user to which the message belongs.

**service information (octet) (SIO)**

*F: octet de service (SER)*

*S: información de servicio (octeto de) (OIS)*

Eight bits, contained in a message signal unit, comprising the service indicator and the sub-service field.

**signal unit (SU)**

*F: trame sémaphore (TS)*

*S: unidad de señalización (US)*

A group of bits forming a separately transferable entity used to convey information on a signalling link.

**signal unit alignment**

*F: alignement des trames sémaphores*

*S: alineación de unidades de señalización*

Signal unit alignment exists when flags are received at intervals which correspond to integral numbers of octets and which fall within certain upper and lower limits.

**signal unit error rate monitoring**

*F: surveillance du taux d'erreur sur les trames sémaphores*

*S: monitor de tasa de errores en las unidades de señalización*

A procedure by which the error rate of an active signalling link is measured on the basis of a count of correctly checking and erroneous signal units.

**signal unit sequence control**

*F: contrôle de l'ordre des trames sémaphores*

*S: control de la secuencia de las unidades de señalización*

Procedures used at level 2 to ensure that message signal units are transported in sequence, without loss or duplication, over a particular signalling link.

**signalling area/network code (SANC)**

*F: code de zone/réseau sémaphore (CZRS)*

*S: código de área/red de señalización*

The field in the international signalling point code that identifies the zone and national signalling area or network. It consists of a code for the world geographical zone (3-bit) and a code for the area or network in a specific zone (8-bit).

**Signalling Connection Control Part (SCCP)**

*F: Sous-Système Commande des connexions Sémaphores (SSCS)*

*S: parte control de la conexión de señalización (PCCS)*

Additional functions to the MTP to cater for both connectionless as well as connection-oriented network service and to achieve an OSI compatible network service.

**signalling information**

*F: information de signalisation*

*S: información de señalización*

The information content of a signal or a signalling message.

**signalling information (field) (SIF)**

*F: information de signalisation (domaine d') (INF)*

*S: información de señalización (campo de) (CIS)*

The bits of a message signal unit which cary information particular to a certain user transaction and always contain a label.

**signalling link**

*F: canal sémaphore*

*S: enlace de señalización*

A transmission means which consists of a signalling data link and its transfer control functions, used for reliable transfer of a signalling message.

**signalling link activation**

*F: activation d'un canal sémaphore*

*S: activación de un enlace de señalización*

The process of making a signalling link ready to carry signalling traffic.

**signalling link blocking**

*F: blocage d'un canal sémaphore*

*S: bloqueo de un enlace de señalización*

An event causing the unavailability of a signalling link, typically consisting in a "processor outage" condition at one end of that signalling link.

**signalling link code (SLC)**

*F: code de canal sémaphore (COC)*

*S: código de enlace de señalización (CES)*

A field of the label in the signalling network management messages, which indicates the particular signalling link to which the message refers among those interconnecting the two involved signalling points.

**signalling link deactivation**

*F: désactivation d'un canal sémaphore*

*S: desactivación de un enlace de señalización*

The procedure by which a signalling link is taken out of service.

**signalling link error monitoring**

*F: surveillance des erreurs sur un canal sémaphore*

*S: monitor de errores en el enlace de señalización*

This comprises two functions: initial alignment error rate monitoring and signal unit error rate monitoring.

**signalling link failure**

*F: défaillance d'un canal sémaphore*

*S: avería (o fallo) del enlace de señalización*

An event causing the unavailability of a signalling link, typically consisting in a failure in signalling terminal equipment or in the signalling data link.

**signalling link group**

*F: groupe de canaux sémaphore*

*S: grupo de enlaces de señalización*

A set of signalling links directly connecting two signalling points and having the same physical characteristics (bit rate, propagation delay, etc.).

**signalling link management functions**

*F: fonctions de gestion des canaux sémaphores*

*S: funciones de gestión de enlaces de señalización*

Functions that control and take actions, when required, to preserve integrity of locally connected signalling links, e.g. by reconfiguration of the signalling link sets.

**signalling link restoration**

*F: rétablissement d'un canal sémaphore*

*S: restauración (o restablecimiento) de enlaces de señalización*

An event consisting in the initial alignment procedure on a signalling link following the removal of the previous causes of failure; if no other causes of unavailability exist (i.e. a signalling link blocked condition) then the signalling link becomes available.

**signalling link selection field**

*F: domaine de sélection du canal sémaphore*

*S: campo de selección de enlace de señalización*

A field of the routing label which is typically used by the message routing function to perform load sharing among different signalling links/link sets.

**signalling link set**

*F: faisceau de canaux sémaphores*

*S: conjunto de enlaces de señalización*

A set of one or more signalling links directly connecting two signalling points.

**signalling link unblocking**

*F: déblocage d'un canal sémaphore*

*S: desbloqueo de un enlace de señalización*

An event consisting in the removal of the previous causes of signalling link blocking; if no other causes of unavailability exist (i.e. a signalling link failed condition), then the signalling link becomes available.

**Signalling Management Application Process (SMAP)**

*F: processus d'application de gestion de signalisation (PAGS)*

*S: proceso de aplicación de gestión de señalización (PAGS)*

The application process associated with the operation, administration, and management of the Signalling System No. 7.

**signalling message**

*F: message de signalisation*

*S: mensaje de señalización*

An assembly of signalling information pertaining to a call, management transaction, etc., that is transferred as an entity.

**signalling message handling functions**

*F: fonctions d'orientation des messages de signalisation*

*S: funciones de tratamiento de mensajes de señalización*

Functions that, at the actual transfer of a message, direct the message to the proper signalling link or User Part.

**signalling network**

*F: réseau sémaphore*

*S: red de señalización*

A network used for signalling by one or more users and consisting of signalling points and connecting signalling links.

**signalling network components**

*F: composants du réseau sémaphore*

*S: componentes de la red de señalización*

Components which make up the signalling network, such as signalling points and common channel signalling links.

**signalling network functions**

*F: fonctions du réseau sémaphore*

*S: funciones de la red de señalización*

The functions which are performed by the Message Transfer Part at level 3 and are common to, and independent of, the operation of individual signalling links. They include the signalling message handling functions and the signalling network management functions.

**signalling end point**

*F: point sémaphore terminal*

*S: punto extremo de señalización*

A node in a signalling network associated with a call originating local exchange, terminating local exchange, or gateway exchange.

**signalling network management functions**

*F: fonctions de gestion du réseau sémaphore*

*S: funciones de gestión de la red de señalización*

Functions that, on the basis of predetermined data and information about the status of the signalling network, control the current message routing and configuration of signalling network facilities.

**signalling point**

*F: point sémaphore*

*S: punto de señalización*

A node in a signalling network which either originates and receives signalling messages, or transfers signalling messages from one signalling link to another, or both.

**signalling point code**

*F: code d'un point sémaphore*

*S: código de punto de señalización*

A binary code uniquely identifying a signalling point in a signalling network. This code is used, according to its position in the label, either as destination point code or as originating point code.

**signalling point numbering plan**

*F: plan de numérotage des points sémaphores*

*S: plan de numeración de los puntos de señalización*

A formal description of the method of translating end-user provided address information into an address understandable by the signalling network.

**signalling point restart**

*F: redémarrage d'un point sémaphore*

*S: rearranque de un punto de señalización*

A procedure that allows a graceful increase of traffic to a restarting node.

**signalling point with SCCP relay function (SPR)**

*F: point sémaphore faisant fonction de relais dans le SSCS (PSR)*

*S: punto de señalización con funciones de relevo PCCS (PSR)*

A node in a signalling network with SCCP relay functions.

**signalling relation**

*F: relation sémaphore*

*S: relación de señalización*

A relation between two signalling points involving the possibility of information interchange between corresponding User Part functions.

**signalling route**

*F: route sémaphore*

*S: ruta de señalización*

A predetermined path described by a succession of signalling points that may be traversed by signalling messages directed by a signalling point towards a specific destination point.

**signalling route management functions**

*F: fonctions de gestion des routes sémaphores*

*S: funciones de gestión de rutas de señalización*

Functions that transfer information about changes in the availability of signalling routes in the signalling network.

**signalling route-set-test procedure**

*F: procédure de test de faisceau de routes sémaphores*

*S: procedimiento de prueba de conjunto de rutas de señalización*

A procedure, included in the signalling route management which is used to test the availability of a given signalling route, previously declared unavailable.

**signalling traffic management functions**

*F: fonctions de gestion du trafic sémaphore*

*S: funciones de gestión del tráfico de señalización*

Functions that control and, when required, modify routing information used by the Message routing function and control the transfer of signalling traffic in a manner that avoids irregularities in the message flow.

**signalling message transfer delay**

*F: temps de transfert d'un message sémaphore*

*S: retardo (tiempo) de transferencia de un mensaje de señalización*

The time a message will take to pass through the signalling network.

**signalling transfer point (STP)**

*F: point de transfert sémaphore (PTS)*

*S: punto de transferencia de señalización (PTS)*

A signalling point with the function of transferring signalling messages from one signallig link to another and considered exclusively from the viewpoint of the transfer.

**status field (SF)**

*F: domaine d'état (ETC)*

*S: campo de estado (CE)*

The bits of a link status signal unit which indicate one of the major signalling link states.

**subservice field (SSF)**

*F: domaine de sous-service (DSS)*

*S: campo de subservicio (CSS)*

The level 3 field containing the network indicator and two spare bits.

**subsystem**

*F: Sous-Système (utilisateur du SSCS)*

*S: subsistema*

A direct user of the Signalling Connection Control Part (SCCP) of Signalling System No. 7.

**subsystem number (SSN)**

*F: numéro de Sous-Système (NSS)*

*S: número de subsistema (NSS)*

A number to identify a subsystem using the SCCP either directly, like the ISDN User Part, or indirectly (via the Transaction Capabilities) like the OMAP.

**system management application entity (SMAE)**

*F: entité d'application de gestion du système (SMAE)*

*S: entidad de aplicación de gestión de sistema (EAGS)*

The aspect of system Management Application Process involved with communication.

**system management application process**

*F: processus d'application de gestion de systèmes*

*S: proceso de aplicación de gestión de sistema*

The set of functions which collectively encompass system management.

**tag (key) (label)**

*F: étiquette (SSGT)*

*S: rótulo (etiqueta)*

The tag distinguishes one information element from another, and governs the interpretation of the contets.

**Telephone User Part (TUP)**

*F: Sous-Système Utilisateur Téléphonie (SSUT)*

*S: parte de usuario de telefonía (PUT)*

The User Part specified for telephone services.

**traffic flow control (signalling-)**

*F: contrôle de flux de trafic (sémaphore)*

*S: control de flujo del tráfico (de señalización)*

Actions and procedures intended to limit signalling traffic at its source in the case when the signalling network is not capable of transferring all signalling traffic offered by the User Parts, because of network failures or overload situations.

**transaction**

*F: transaction*

*S: transacción*

An association between two TC providers.

**Transaction Capabilities (TC)**

*F: Gestionnaire de Transactions (GT)*

*S: capacidades de transacción (CT)*

Functions which control information transfer between two or more nodes via a signalling network.

**Transaction Capabilities Application Part (TCAP)**

*F: Sous-Système application pour la Gestion des Transactions (SSGT)*

*S: parte aplicación de capacidades de transacción (PACT)*

The part of the Transaction Capabilities that resides in the application layer of the OSI protocol references model.

**transaction portion**

*F: partie transaction*

*S: porción de transacción*

The portion of the TCAP message that identifies whether the transaction is expected to consist of single or multiple messages and provides a means to associate these messages with a specific transaction and to terminate a transaction. The part of TCAP messages dealing with the control of transactions.

**transceiver**

*F: émetteur-récepteur*

*S: transceptor (transmisor-receptor)*

A tone device inserted in the outgoing end of a circuit which performs the transmitter and receiver check test through a check loop.

**transfer-allowed (procedure)**

*F: transfert autorisé (procédure de)*

*S: autorización de transferencia (procedimiento de)*

A procedure, included in the signalling route management, which is used to inform a signalling point that a signalling route has become available.

**transfer controlled (procedure)**

*F: transfert sous contrôle (procédure de)*

*S: control de transferencia (procedimiento de)*

A procedure, included in signalling route management, which does inform a signalling point of the congestion status of a signalling route.

**transfer-prohibited (procedure)**

*F: transfert interdit (procédure de)*

*S: prohibición de transferencia (procedimiento de)*

A procedure, included in the signalling route management, which is used to inform a signalling point of the unavailability of a signalling route.

**transfer restricted (procedure)**

*F: transfert restreint (procédure de)*

*S: restricción de transferencia (procedimiento de)*

A procedure, included in signalling route management, which does inform a signalling point of the restriction of a signalling route.

**transmission buffer (TB)**

*F: tampon d'émission (TEM)*

*S: memoria tampón de transmisión (MT)*

Storage in the signalling link control for message signal units not yet transmitted.

**user (of the signalling system)**

*F: utilisateur du système de signalisation*

*S: usuario (del sistema de señalización)*

A functional entity, typically a telecommunication service, which uses a signalling network to transfer information.

**User Part (UP)**

*F: Sous-Système Utilisateur (SSU)*

*S: parte de usuario (o parte de usuario) (PU)*

A functional part of the common channel signalling system which transfers signalling messages via the Message Transfer Part. Different types of User Parts exist (e.g. for telephone and data services), each of which is specified to a particular use of the signallig system.

## ABBREVIATIONS SPECIFIC TO SIGNALLING SYSTEM No. 7 [1]

| English | French | Spanish | Meaning |
|---|---|---|---|
| ACB | ACI | SAP | Access barred signal<br>Table 3/Q.723 |
| ACC | RAE | CAC | Automatic congestion control information message<br>Table 3/Q.723 |
| ACM | ACO | MDC | Address complete message<br>Table 3/Q.723, Figure 3/Q.724 |
| ADI | ADI | SDI | Address incomplete signal<br>Table 3/Q.723, Figure 3/Q.724 |
| AERM | STEA | MA | Alignment error rate monitor<br>Figures 7-9/Q.703 and 11-17/Q.703 |
| ANC | RAT | RCT | Answer signal, charge<br>Table 3/Q.723, Figure 3/Q.724 |
| ANN | RST | RST | Answer signal, no charge<br>Table 3/Q.723 |
| ANU | RSI | RNC | Answer signal, unqualified<br>Table 3/Q.723 |
| BIB | BIR | BII | Backward indicator bit<br>Figures 3/Q.703, 13/Q.703 and 15/Q.703 |
| BLA | BLA | ARB | Blocking-acknowledgement signal<br>Table 3/Q.723 |
| BLO | BLO | BLO | Blocking signal<br>Table 3/Q.723 |
| BSM | DE | MPE | Backward set-up message<br>Table 3/Q.723 |
| BSN | NSR | NSI | Backward sequence number<br>Figures 3/Q.703, 14/Q.703 and 16/Q.703 |
| BSNR | NSR-R | NSIR | Backward sequence number received<br>Figures 7/Q.703, 13/Q.703, 14/Q.703, 16/Q.703 |
| BSNT | NSR-E | NSIT | Backward sequence number of next SU to be transmitted<br>Figures 7-9/Q.703 and 13-16/Q.703, Figures 27 and 30/Q.704. |
| CBA | RCA | ARS | Changeback acknowledgement signal<br>Table 3/Q.704 |
| CBD | RCO | ORS | Changeback declaration signal<br>Table 3/Q.704 |
| CBK | RAC | COL | Clear-back signal<br>Table 3/Q.723, Figure 3/Q.724 |
| CCF | CCN | FCO | Continuity-failure signal<br>Table 3/Q.723 |

[1] This list of abbreviations is basically the one appearing in Fasicle VI.6 of the *Yellow Book*, 1980. Study Group XI should bring this list up to date in the Study Period 1989-1992.

| English | French | Spanish | Meaning |
|---|---|---|---|
| CCI | CCE | PCL | Continuity check incoming<br>Recommendation Q.724, § 7.3, Figures 3/Q.724, 5/Q.724 |
| CCL | RAD | LALN | Calling party clear signal<br>Table 3/Q.723 |
| CCM | SC | MSC | Circuit supervision message<br>Table 3/Q.723 |
| CCO | CCS | PCS | Continuity-check outgoing<br>Recommendation Q.723, § 7.3, Figures 3/Q.724, 4/Q.724 |
| CCR | CCD | PPC | Continuity-check-request signal<br>Table 3/Q.723, Figures 2/Q.724, 3/Q.724, 6/Q.724 and 7/Q.724 |
| CCS | CS | SCC | Common channel signalling<br>Recommendation Q.701, § 1.1 |
| CFL | ECH | SLI | Call-failure signal<br>Table 3/Q.723, Figure 3/Q.724 |
| CGC | EFC | CHC | Circuit-group-congestion<br>Table 3/Q.723, Figure 3/Q.724 |
| CHG | TAX | MTA | Charging message<br>Table 3/Q.723 |
| CHM | PR | MPA | Changeover and changeback messages<br>Table 1/Q.704 |
| CIC | CIC | CIC | Circuit identification code<br>Recommendation Q.704, § 15, Recommendation Q.723, § 2.2.1 |
| CIR | IDD | PIL | Calling-line-identity-request signal<br>Table 3/Q.723 |
| CK | CRT | BCE | Check bits<br>Figure 3/Q.703 |
| CLF | FIN | FIN | Clear-forward signal<br>Table 3/Q.723, Figures 3/Q.724, 6/Q.724, 7/Q.724 |
| CNM | GRC | GRC | Circuit network management message group |
| CNP | CLI | CIM | Connection-not-possible signal<br>Table 1/Q.704 |
| CNS | CLN | CIN | Connection-not-successful signal<br>Table 1/Q.704 |
| COA | PCA | APR | Changeover acknowledgement signal<br>Table 1/Q.704 |
| COO | PCO | OPR | Changeover order signal<br>Table 1/Q.704 |
| COT | CCP | CON | Continuity signal<br>Table 3/Q.723, Figure 3/Q.724 |
| CPC | STA | CTL | Call processing control<br>Recommendation Q.724, § 10.2, Figures 1-7/Q.724 |
| CRI | CRE | RPL | Continuity recheck incoming<br>Recommendation Q.724, § 15.1, Figures 1/Q.724, 2/Q.724, 3/Q.724, 6/Q.724, 7/Q.724 |
| CRO | CRS | RPS | Continuity-recheck outgoing<br>Recommendation Q.724, § 15.1, Figures 1-3/Q.724, 6/Q.724 |
| CSM | SA | MSL | Call supervision message<br>Table 3/Q.723 |
| CSS | CLR | SCF | Connection-successful signal<br>Table 1/Q.704 |
| DAEDR | DAD-R | DADR | Delimitation, alignment, error detection (reception)<br>Figures 7/Q.703, 9/Q.703, 11/Q.703, 14/Q.703, 16/Q.703, 17/Q.703, 18/Q.703 |
| DAEDT | DAD-E | DADT | Delimitation, alignment, error detection (transmitting)<br>Figures 12/Q.703, 13/Q.703, 15/Q.703 |

| English | French | Spanish | Meaning |
|---|---|---|---|
| DCE | ETCD | ETCD | Data circuit terminating equipment<br>Figure 1/Q.702 |
| DLC | CLO | CED | Signalling-data-link-connection-order signal<br>Table 1/Q.704 |
| DLM | CL | MED | Signalling-data-link-connection-order message<br>Table 1/Q.704 |
| DPC | CPD | CPD | Destination point code<br>Recommendation Q.704, §§ 2.2.3, 13.2, Figure 3/Q.704, 14/Q.704, 26/Q.704, Recommendation Q.706, § 3, Recommendation Q.723, § 2.2.1 |
| DPN | CNN | TDN | Digital path not provided signal<br>Table 3/Q.723 |
| DUP | SSUD | PUD | Data user part<br>Recommendation Q.701, § 2.1, Figure 2/Q.701 |
| ECA | PUA | AER | Emergency changeover acknowledgement signal<br>Table 1/Q.704 |
| ECM | PU | MEP | Emergency changeover message<br>Table 1/Q.704 |
| ECO | PUO | PER | Emergency changeover order signal<br>Table 1/Q.704 |
| EUM | EXT | IAL | Extended-unsuccessful-backward set-up information message indication<br>Table 3/Q.723 |
| F | F | BAN | Flag<br>Figure 3/Q.703 |
| FAM | AD | MDA | Forward-address message<br>Table 3/Q.723 |
| FCM | CF | MCF | Signalling traffic flow control messages<br>Table 1/Q.704 |
| FDM | MRF | MDF | Frequency division multiplex<br>Recommendation Q.723, § 2.2.3, Recommendation Q.724, § 9 |
| FIB | BIA | BID | Forward indicator bit<br>Figures 3/Q.703, 13/Q.703, 15/Q.703 |
| FISU | TSR | USR | Fill-in signal unit<br>Figures 7/Q.703, 8/Q.703, 13-16/Q.703 |
| FOT | IOP | INT | Forward-transfer signal<br>Table 3/Q.723 |
| FSM | EA | MEL | Forward set-up message<br>Table 3/Q.723 |
| FSN | NSA | NSD | Forward sequence number<br>Figures 3/Q.703, 13/Q.703 |
| GRA | RZA | ARG | Circuit group reset-acknowledgement message<br>Table 3/Q.723 |
| GRM | SGC | MSG | Circuit group supervision message<br>Table 3/Q.723 |
| GRQ | DEG | MPG | General request message |
| GRS | RZG | MRG | Circuit group reset message<br>Table 3/Q.723 |
| GSM | ING | MEG | General forward setup information message |

| English | French | Spanish | Meaning |
|---|---|---|---|
| HBA | BHA | ABGSF | Hardware failure oriented group blocking-acknowledgement message<br>Table 3/Q.723 |
| HGB | BLH | BGSF | Hardware failure oriented group blocking message<br>Table 3/Q.723 |
| HGU | DBH | DGSF | Hardware failure oriented group unblocking message<br>Table 3/Q.723 |
| HUA | DHA | ADGSF | Hardware failure oriented group unblocking acknowledgement message<br>Table 3/Q.723 |
| HMDC | ODC | HDCM | Message discrimination<br>Recommendation Q.704, § 2, Figures 23-26/Q.704 |
| HMDT | ODT | HDTM | Message distribution<br>Recommendation Q.704, § 2, Figures 23-25/Q.704, 28/Q.704, 30/Q.704, 31/Q.704, 42/Q.704, 44-46/Q.704, 2/Q.707 |
| HMRT | OAC | HENM | Message routing<br>Recommendation Q.704, § 2, Figures 23/Q.704, 24/Q.704, 26/Q.704, 27/Q.704, 30/Q.704, 31/Q.704, 32/Q.704, 33/Q.704, 42/Q.704, 44/Q.704, 45/Q.704, 46/Q.704, 2/Q.707 |
| HO | HO | EO | Heading code<br>Recommendation Q.704, § 15.3, Figure 16/Q.704, Recommendation Q.707, § 5.3, Figure 1/Q.707, Recommendation Q.723, §§ 3.1 and 3.2 |
| H1 | H1 | E1 | Heading code<br>Recommendation Q.704, § 15.3, Figure 16/Q.704, Recommendation Q.723, § 3.1 |
| IAC | CAI | CAI | Initial alignment control<br>Figures 8/Q.703, 9/Q.703, 13-17/Q.703 |
| IAI | MIS | MIA | Initial address message with additional information<br>Table 3/Q.723 |
| IAM | MIA | MID | Initial address message<br>Table 3/Q.723, Figures 3/Q.724, 6/Q.724 |
| ISDN-UP (ISUP) | SSUR | PU-RDSI | ISDN User Part<br>Recommendations Q.700 and Q.761 to Q.764 |
| ISP | PSI | PSI | International signalling point<br>Recommendation Q.705, § 3, Figure 1/Q.705 |
| L1 | N1 | N1 | Level 1<br>Figures 12/Q.703, 35/Q.704, 38-40/Q.704 |
| L2 | N2 | N2 | Level 2<br>Figures 8/Q.703, 9/Q.703, 12/Q.703, 13/Q.703, 15/Q.703, 23/Q.704, 24/Q.704, 26/Q.704, 27/Q.704, 30/Q.704, 35/Q.704, 37/Q.704 |
| L3 | N3 | N3 | Level 3<br>Figures 8/Q.703, 9/Q.704, 13/Q.703, 15/Q.703, 23/Q.704, 24/Q.704, 26/Q.704, 30/Q.704, 31/Q.704, 34/Q.704, 35/Q.704, 37/Q.704, 38/Q.704, 39/Q.704 |
| L4 | N4 | N4 | Level 4<br>Figures 23/Q.704, 25-27/Q.704, 34/Q.704 |
| LI | INL | IL | Length indicator<br>Recommendation Q.703, § 2.2, Figure 3/Q.703 |
| LLSC | GCSF | CCE | Link set control<br>Figures 29/Q.704, 35-37/Q.704 |
| LOS | LHS | LFS | Line-out-of-service signal<br>Table 3/Q.723, Figure 3/Q.724 |
| LSAC | GCSA | CAE | Signalling link activity control<br>Recommendation Q.704, § 12.6, Figures 28-30/Q.704, 35-41/Q.704 |
| LSC | SET | CEE | Link state control<br>Figures 7-10/Q.703, 13-18/Q.703, Recommendation Q.704, § 14.6, Figure 41/Q.704 |

| English | French | Spanish | Meaning |
|---|---|---|---|
| LSDA | GCAL | AED | Signalling data link allocation<br>Recommendation Q.704, § 12.6, Figures 35/Q.704, 37-40/Q.704, 42/Q.704 |
| LSLA | GCAC | AES | Signalling link activation<br>Recommendation Q.704, § 12.6, Figures 35/Q.704, 37/Q.704, 38/Q.704, 41/Q.704, 42/Q.704 |
| LSLD | GCDA | DES | Signalling link deactivation<br>Recommendation Q.704, § 12.6, Figures 35/Q.704, 37/Q.704, 40/Q.704, 41/Q.704, 42/Q.704 |
| LSLR | GCRE | RES | Signalling link restoration<br>Recommendation Q.704, § 12.6, Figures 35/Q.704, 37/Q.704, 39/Q.704, 41/Q.704, 42/Q.704 |
| LSSU | TSE | UEE | Link status signal units<br>Figures 13-16/Q.703 |
| LSTA | GCAT | ATS | Signalling terminal allocation<br>Recommendation Q.704, § 12.6, Figures 35/Q.704, 38/Q.704, 39/Q.704, 40/Q.704, 41/Q.704 |
| MBA | BMA | ABGM | Maintenance oriented group-blocking-acknowledgement<br>Table 3/Q.723 |
| MGB | BLM | BGM | Maintenance oriented group blocking message<br>Table 3/Q.723 |
| MGMT | GES | SGE | Management system<br>Figures 8/Q.703, 27/Q.704, 28/Q.704, 35-37/Q.704, 2/Q.707 |
| MGU | DBM | DGM | Maintenance oriented group unblocking message<br>Table 3/Q.723 |
| MPR | INU | PIMM | Misdialled trunk prefix<br>Table 3/Q.723 |
| MSU | TSM | USM | Message signal unit<br>Recommendation Q.701, § 2.3, Figures 7/Q.703, 8/Q.703, 14/Q.703, 15/Q.703, 16/Q.703 |
| MTP | SSTM | PTM | Message transfer part<br>Recommendation Q.701, § 2.1, Recommendation Q.721, § 1 |
| MUA | DMA | ADGM | Maintenance oriented group unblocking-acknowledgement message<br>Table 3/Q.723 |
| NACK | ACN | RN | Negative acknowledgement<br>Figures 7/Q.703, 13/Q.703, 14/Q.703 |
| NNC | ERN | CRN | National-network-congestion signal<br>Table 3/Q.723, Figure 3/Q.724 |
| NSP | PSN | PSN | National signalling point<br>Recommendation Q.705, § 3, Figure 1/Q.705 |
| OMAP | SSEM | POMA | Operation, Administration and Maintenance Part<br>Recommendations Q.700 and Q.795 |
| OPC | CPO | CPO | Originating point code<br>Recommendation Q.704, §§ 2.2.3 and 13.2, Figures 3/Q.704 and 14/Q.704, Recommendation Q.706, § 3, Recommendation Q.723, § 2.2.1 |
| PCM | MIC | MIC | Pulse code modulation<br>Recommendation Q.702, § 5.3 |
| PCR | RCP | RCP | Preventive cyclic retransmission<br>Tables 1/Q.706, 2/Q.706 |

| English | French | Spanish | Meaning |
|---|---|---|---|
| POC | SIP | CIP | Processor outage control<br>Figures 8/Q.703, 10/Q.703 |
| RAN | NRP | RRE | Reanswer signal<br>Table 3/Q.723, Figure 3/Q.724 |
| RC | REC | CR | Reception control<br>Figures 8/Q.703, 9/Q.703, 11/Q.703, 13-16/Q.703 |
| RLG | LIG | LGU | Release-guard signal<br>Table 3/Q.723, Figures 2/Q.724, 3/Q.724, 6/Q.724, 7/Q.724 |
| RSC | RZC | RCI | Reseat-circuit signal<br>Table 3/Q.723 |
| RSM | TR | MPR | Signalling-route-set-test message<br>Table 1/Q.704 |
| RSRT | GRTF | CPC | Signalling route set test control<br>Recommendation Q.704, § 13.5, Figures 23/Q.704, 29/Q.704, 43-46/Q.704 |
| RST | TRS | PRS | Signalling-route-set-test signal<br>Table 1/Q.704 |
| RTAC | GRTA | CTA | Transfer allowed control<br>Recommendation Q.704, § 13.3, Figures 29/Q.704, 33/Q.704, 37/Q.704, 43/Q.704, 45/Q.704, 46/Q.704 |
| RTB | TRT | MTR | Retransmission buffer<br>Figures 7/Q.703, 13/Q.703, 15/Q.703 |
| RTPC | GRTI | CTP | Transfer prohibited control<br>Recommendation Q.704, § 13.2, Figures 26/Q.704, 29/Q.704, 32/Q.704, 43/Q.704, 44/Q.704, 46/Q.704 |
| SAM | MSA | MSD | Subsequent-address message<br>Table 3/Q.723, Figure 3/Q.724 |
| SAO | MSS | SDU | Subsequent-address message with one signal<br>Table 3/Q.723 |
| SBA | BSA | ABGSL | Software generated group blocking-acknowledgement message<br>Table 3/Q.723 |
| SBM | SE | MEC | Successful-backward-set-up information message<br>Table 3/Q.723 |
| SCCP | SSCS | PCCS | Signalling Connection Control Part<br>Recommendations Q.700, Q.711-Q.714 and Q.716 |
| SDL | LDS | LED | Functional specification and description language<br>Recommendations Q.703, § 12, Q.704, § 6, Q.707, Recommendations Q.714, Q.724, Q.764, Q.774 |
| SEC | EEC | CEC | Switching-equipment-congestion signal<br>Table 3/Q.723, Figure 3/Q.724 |
| SF | ETC | CE | Status field<br>Figure 3/Q.703 |
| SGB | BLS | BGSL | Software generated group blocking message<br>Recommendation Q.723, Table 3/Q.723 |
| SGU | DBS | DGSL | Software generated group unblocking message<br>Recommendation Q.723, Table 3/Q.723 |
| SI | INS | IS | Service indicator<br>Recommendation Q.704, § 14 |
| SIE | ETAU | IAE | Status indication "emergency terminal status"<br>Recommendation Q.703, §§ 7.2, 7.3 and 10.1.3, Figures 2/Q.703, 4/Q.703, 7-9/Q.703, 13-16/Q.703 |
| SIF | INF | CIS | Signal information field<br>Figure 3/Q.703 |
| SIN | ETAN | IAN | Status indication "normal terminal status"<br>Recommendation Q.703, §§ 7.2, 7.3 and 10.1.3, Figures 2/Q.703, 4/Q.703, 7-9/Q.703, 13-16/Q.703 |
| SIO | SER | OIS | Service information octet<br>Figure 3/Q.703, Recommendation Q.723, § 1.2 |

| English | French | Spanish | Meaning |
|---|---|---|---|
| SIO [2] | ETAP | IFA | Status indication "out of alignment"<br>Recommendation Q.703, §§ 7.2, 7.3 and 10.1.3, Figures 2/Q.703, 4/Q.703, 7-9/Q.703, 13-16/Q.703 |
| SIOS | ETHS | IFS | Status indication "out of service"<br>Recommendation Q.703, §§ 7.2, 7.3 and 10.1.3, Figures 2/Q.703, 4/Q.703, 7-9/Q.703, 13-16/Q.703 |
| SIPO | ETIP | IIP | Status indication "processor outage"<br>Recommendation Q.703, § 10.1.3, Figures 2/Q.703, 7/Q.703, 8/Q.703, 13-16/Q.703 |
| SLC | COC | CES | Signalling link code<br>Recommendation Q.704, § 15, Figure 14/Q.704 |
| SLM | GCS | GES | Signalling link management<br>Recommendation Q.704, §§ 12.1 and 12.6, Figures 23/Q.704, 25/Q.704, 26/Q.704, 27/Q.704, 29/Q.703 |
| SLS | SCS | SES | Signalling link selection code<br>Recommendation Q.704, § 2.2.4, Figures 3/Q.704, 4/Q.704, 26/Q.704, A-3.1/Q.705 |
| SLTA | ESCA | AMPS | Signalling link test message acknowledgement |
| SLTM | ESCO | MPES | Signalling link test message<br>Figure 2/Q.707 |
| SMH | OMS | TMS | Signalling message handling<br>Recommendation Q.704, § 2, Figures 23/Q.704, 43/Q.704 |
| SP | PS | PS | Signalling point<br>Figures 8/Q.704, 23/Q.704, 24/Q.704, 26/Q.704, 27/Q.704, 30/Q.704, 31/Q.704, 42-44/Q.704 |
| SPRC | CPS | CPS | Signalling procedure control<br>Recommendation Q.724, § 10.1, Figures 1-7/Q.724 |
| SRM | GRS | GRS | Signalling route management<br>Recommendation Q.704, § 13, Figures 23/Q.704, 25-27/Q.704, 43/Q.704 |
| SSB | OCC | ABO | Subscriber-busy signal (electrical)<br>Table 3/Q.723, Figure 3/Q.724 |
| SSF | DSS | CSS | Sub-service field<br>Recommendation Q.704, § 13.1.1, Recommendation Q.723, § 1.2 |
| SST | TSI | TIE | Send-special-information-tone signal<br>Figures 1-7/Q.724 |
| ST | ST | SFN | End-of-pulsing signal<br>Recommendation Q.724, § 1.3 |
| STLC | ESC | CPES | Signalling link test control<br>Figures 25/Q.704, 26/Q.704, 2/Q.707 |
| STM | GTS | GTS | Signalling traffic management<br>Recommendation Q.704, § 4, Figures 23/Q.704, 25-27/Q.704, 30/Q.704, 35/Q.704, 39/Q.704, 43/Q.704 |
| STP | PTS | PTS | Signalling transfer point<br>Figure 4/Q.701, Recommendation Q.705, § 3, Figures A-1/Q.705, A-2/Q.705, Recommendation Q.706, § 4.3.3, Table 3/Q.706 |
| SU | TS | US | Signal unit<br>Figures 2/Q.703, 7/Q.703 |
| SUA | DSA | ADGSL | Software generated group unblocking-acknowledgement messages<br>Table 3/Q.723 |

[2] In English, another abbreviation will have to be found for *status indication "out of alignment"*, since the abbreviation SIO is already used for *service information octet*

| English | French | Spanish | Meaning |
|---|---|---|---|
| SUERM | STTS | MUS | Signal unit error rate monitor<br>Figures 7/Q.703, 8/Q.703, 11/Q.703, 18/Q.703 |
| SUM | SEE | ESNC | Sample unsuccessful backward setup information message<br>Recommendation Q.723, § 3.7.1 |
| TB | TEM | MT | Transmission buffer<br>Figures 7/Q.703, 13/Q.703, 15/Q.703 |
| TC | GT | CT | Transaction Capabilities<br>Recommendations Q.700 and Q.771-Q.775 |
| TCAP | SSGT | PACT | Transaction Capabilities Application Part<br>Recommendations Q.700 and Q.771-Q.775. |
| TCBC | GTCN | TCRS | Changeback control<br>Recommendation Q.704, § 6, Figures 27-29/Q.704, 31/Q.704 |
| TCOC | GTCS | TCER | Changeover control<br>Recommendation Q.704, § 5, Figures 27-30/Q.704, 37/Q.704 |
| TCRC | GTRN | TCRC | Controlled rerouting control<br>Recommendation Q.704, § 8, Figures 27/Q.704, 29/Q.704, 33/Q.704, 45/Q.704 |
| TFA | TAO | TRA | Transfer-allowed signal<br>Table 1/Q.704 |
| TFM | TF | MTR | Transfer-prohibited and transfer-allowed messages<br>Table 1/Q.704 |
| TFP | TIO | PTR | Transfer-prohibited signal<br>Table 1/Q.704 |
| TFRC | GTRS | TCRF | Forced rerouting control<br>Recommendation Q.704, § 7, Figures 27/Q.704, 29/Q.704, 32/Q.704 |
| TLAC | GTSD | TCDE | Link availability control<br>Recommendation Q.704, Figures 27-31/Q.704, 37/Q.704 |
| TSFC | GTFX | CFTS | Signalling traffic flow control<br>Figures 27/Q.704, 29/Q.704, 34/Q.704 |
| TSRC | GTAC | CEN | Signalling routing control<br>Recommendation Q.704, Figures 27-34/Q.704, 36/Q.704, 37/Q.704, 44-46/Q.704 |
| TUP | SSUT | PUT | Telephone user part<br>Recommendation Q.701, § 2.1, Figure 2/Q.701, Recommendation Q.721, § 1 |
| TXC | EMI | CT | Transmission control<br>Figures 8/Q.703, 9/Q.703, 12-16/Q.703 |
| UBA | DBA | ARD | Unblocking-acknowledgement signal<br>Table 3/Q.723 |
| UBL | DBO | DBL | Unblocking signal<br>Table 3/Q.723 |
| UBM | EE | MEI | Unsuccessful-backward-set-up-information message<br>Table 3/Q.723 |
| UNN | NNU | NNA | Unallocated-national-number signal<br>Table 3/Q.723, Figure 3/Q.724 |
| UP | SSU | PU | User part<br>Figure 2/Q.704 |

ISBN 92-61-03511-6