INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

G.784

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(06/99)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital transmission systems – Terminal equipments – Principal characteristics of multiplexing equipment for the synchronous digital hierarchy

Synchronous Digital Hierarchy (SDH) management

ITU-T Recommendation G.784

(Previously CCITT Recommendation)

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
INTERNATIONAL ANALOGUE CARRIER SYSTEM	
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	
TRANSMISSION MEDIA CHARACTERISTICS	
DIGITAL TRANSMISSION SYSTEMS	
TERMINAL EQUIPMENTS	G.700–G.799
General	G.700–G.709
Coding of analogue signals by pulse code modulation	G.710–G.719
Coding of analogue signals by methods other than PCM	G.720–G.729
Principal characteristics of primary multiplex equipment	G.730–G.739
Principal characteristics of second order multiplex equipment	G.740–G.749
Principal characteristics of higher order multiplex equipment	G.750–G.759
Principal characteristics of transcoder and digital multiplication equipment	G.760–G.769
Operations, administration and maintenance features of transmission equipment	G.770–G.779
Principal characteristics of multiplexing equipment for the synchronous digital hierarchy	**G.780–G.789**
Other terminal equipment	G.790–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION G.784

SYNCHRONOUS DIGITAL HIERARCHY (SDH) MANAGEMENT

Summary

This Recommendation addresses management aspects of the synchronous digital hierarchy (SDH), including the control and monitoring functions relevant to SDH network elements (NE). The SDH management subnetwork (SMS) architecture, SDH embedded control channel (ECC) functions, and SDH ECC protocols are specified. Detailed message sets are for further study.

The management of SDH equipment should be seen as a subset of the telecommunications management network (TMN) described in Recommendation M.3000, and reference is made to Recommendation G.773 for the specification of protocol suites to be used at external (Q) management interfaces.

This Recommendation specifies for fault management, performance monitoring, and configuration management a library of basic equipment management function (EMF) building blocks and a set of rules by which they are combined in order to describe a digital transmission equipment's EMF functionality. The library defined in this Recommendation forms part of the set of libraries defined furthermore in Recommendation G.783.

Not every function defined in this Recommendation is required for every application. Different subsets of functions may be assembled in different ways to provide a variety of different capabilities. Network operators and equipment suppliers may choose which functions must be implemented for each application.

Source

ITU-T Recommendation G.784 was revised by ITU-T Study Group 15 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 22nd of June 1999.

History

Issue	Notes
06/99	Second revision: Modifications are made to clauses 1, 4 (previous 2.1), 3 (previous 2.2), Table 8-3 (previous Table 6-3), and References. The previous clause 5 and Annex A are deleted and replaced by new text in clause 7 and Annex A. Annex D is deleted. Appendix I is added. Modifications are made to align with Recommendation A.3. Clauses 3 to 8 are renumbered into clauses 5 to 10. The References part is moved into clause 2, Definitions into clause 3 and Abbreviations into clause 4. Summary is added and Scope in clause 1 is extended. List of abbreviations in clause 4 is extended.
01/94	First revision
1990	Initial version

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation the term *recognized operating agency (ROA)* includes any individual, company, corporation or governmental organization that operates a public correspondence service. The terms *Administration, ROA* and *public correspondence* are defined in the *Constitution of the ITU (Geneva, 1992)*.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Recommendation G.784

SYNCHRONOUS DIGITAL HIERARCHY (SDH) MANAGEMENT

(revised in 1994 and 1999)

1 Scope

This Recommendation addresses management aspects of the synchronous digital hierarchy (SDH), including the control and monitoring functions relevant to SDH network elements (NE). The SDH management subnetwork (SMS) architecture, SDH embedded control channel (ECC) functions, and SDH ECC protocols are specified. Detailed message sets are for further study.

The management of SDH equipment should be seen as a subset of the telecommunications management network (TMN) described in Recommendation M.3000, and reference is made to Recommendation G.773 for the specification of protocol suites to be used at external (Q) management interfaces.

This Recommendation specifies for fault management, performance monitoring, and configuration management a library of basic equipment management function (EMF) building blocks and a set of rules by which they are combined in order to describe a digital transmission equipment's EMF functionality. The library defined in this Recommendation forms part of the set of libraries defined furthermore in Recommendation G.783.

Not every function defined in this Recommendation is required for every application. Different subsets of functions may be assembled in different ways to provide a variety of different capabilities. Network operators and equipment suppliers may choose which functions must be implemented for each application.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ISO 8473:1988, *Information processing systems – Data communications – Protocol for providing the connectionless-mode network service*.

[2] ISO 8473:1988/Add.3:1989, *Information processing systems – Data communications – Protocol for providing the connectionless-mode network service – Addendum 3: Provision of the underlying service assumed by ISO 8473 over subnetworks which provide the OSI data link service.*

[3] ISO/IEC 8073:1988/Add.2, *Information processing systems – Open Systems Interconnection – Connection oriented transport protocol specification – Addendum 2: Class 4 operation over connectionless network service.*

[4] ISO/IEC 9596:1991, *Information technology – Open Systems Interconnection – Common management information service definition*.

[5] ITU-T Recommendation Q.920 (1993), *ISDN user-network interface data link layer – General aspects.*

[6] ITU-T Recommendation Q.921 (1997), ISDN user-network interface – Data link layer specification.

[7] ITU-T Recommendation Q.811 (1993), *Lower layer profiles for the Q3 interface*.

[8] ITU-T Recommendation Q.812 (1993), *Upper layer profiles for the Q3 interface*.

[9] CCITT Recommendation X.212 (1988), *Data link service definition for Open Systems Interconnection for CCITT applications.*

ISO/IEC 8886:1992, *Information technology – Telecommunications and Information exchange between systems – Data link service definition for Open Systems Interconnection.*

[10] CCITT Recommendation Q.922 (1992), *ISDN data link layer specification for frame mode bearer services*.

[11] ITU-T Recommendation G.783 (1997), *Characteristics of Synchronous Digital Hierarchy (SDH) equipment functional blocks*.

[12] CCITT Recommendation G.774 (1992), *Synchronous Digital Hierarchy (SDH) management information model for the network element view*.

3 Definitions

This Recommendation defines the following terms:

3.1 data communications channel (DCC): Within an STM-N signal there are two DCC channels, comprising bytes D1-D3, giving a 192 kbit/s channel, and bytes D4-D12, giving a 576 kbit/s channel. D1-D3 (DCC_R) are accessible by all SDH NEs whereas D4-D12 (DCC_M), not being part of the regenerator section overhead, are not accessible at regenerators. It is recommended to have both DCC_M and DCC_R available in backbone STM-16 (and higher order) network sections. DCC_M is used to forward data over the multiplex sections (using the OSI-routing protocols), and DCC_R is used to forward data to the regenerators within the destination MS span. DCC_M can be regarded as the backbone, while DCC_R and LAN are used to interconnect this backbone to equipment that cannot be accessed through DCC_M, e.g. regenerators and non-SDH equipment.

DCC_M and DCC_R can be used to carry two independent, possibly proprietary management applications. An NE can choose to throughconnect DCC_M on the physical level, or to terminate the DCC_M and route the PDUs, while using the DCC_R for interconnection within a subnetwork.

3.2 embedded control channel (ECC): An ECC provides a logical operations channel between SDH NEs, utilizing a data communications channel (DCC) as its physical layer.

3.3 SDH management network (SMN): An SDH management network is a subset of a TMN, responsible for managing SDH NEs. An SMN may be subdivided into a set of SDH management subnetworks.

3.4 SDH management subnetwork (SMS): An SDH management subnetwork (SMS) consists of a set of separate SDH ECCs and associated intra-site data communication links which have been interconnected to form an operations data communications control network within any given SDH transport topology. An SMS represents an SDH specific local communications network (LCN) portion of a network operator's overall operations data network or TMN.

3.5 management applications function (MAF): An application process participating in system management. The management applications function includes an agent (being managed) and/or manager. Each SDH network element (NE) and operations system or mediation device (OS/MD) must support a management application function that includes at least an agent. A management application function is the origin and termination for all TMN messages.

3.6 **manager**: Part of the MAF which is capable of issuing network management operations (i.e. retrieve alarm records, set thresholds) and receiving events (i.e. alarms, performance). SDH NEs may or may not include a manager while SDH OS/MDs will include at least one manager.

3.7 **agent**: Part of the MAF which is capable of responding to network management operations issued by a manager and may perform operations on managed objects, issuing events on behalf of managed objects. The managed objects can reside within the entity or in another open system. Managed objects from other open systems are controlled by a distant agent via a local manager. All SDH NEs will support at least an agent. Some SDH NEs will provide managers and agents (being managed). Some NEs (e.g. regenerators) will only support an agent.

3.8 **managed object (MO)**: The management view of a resource within the telecommunication environment that may be managed via the agent. Examples of SDH managed objects are: equipment, receive port, transmit port, power supply, plug-in card, virtual container, multiplex section and regenerator section.

3.9 **managed object class (MOC)**: An identified family of managed objects that share the same characteristics, e.g. "equipment" may share the same characteristics as "plug-in card".

3.10 **message communications function (MCF)**: The message communications function provides facilities for the transport of TMN messages to and from the MAF, as well as facilities for the transit of messages. The message communications function does not originate or terminate messages (in the sense of the upper protocol layers).

3.11 **operations system function or mediation function (OSF/MF)**: A telecommunications management network (TMN) entity that processes management information to monitor and control the SDH network. In the SDH sub-portion of the TMN, no distinction is made between the operations system function and the mediation function; this entity being a MAF containing at least a manager.

3.12 **network element function (NEF)**: A function within an SDH entity that supports the SDH based network transport services, e.g. multiplexing, cross-connection, regeneration. The network element function is modelled by managed objects.

3.13 **operations system or mediation device (OS/MD)**: A stand-alone physical entity that supports OSF/MFs but does not support NEFs. It contains a message communication function (MCF) and a MAF.

3.14 **network element (NE)**: A stand-alone physical entity that supports at least NEFs and may also support OSF/MFs. It contains managed objects, a MCF and a MAF.

3.15 **trail segment**: A segment for which one end is a trail termination.

4 Abbreviations

This Recommendation uses the following abbreviations:

ACSE	Association control service element
AcSL	Accepted Signal Label
AcTI	Accepted Trace Identifier
AF	Application Function
AF	Atomic Function
AIS	Alarm Indication Signal
AITS	Acknowledged information transfer service
AP	Access Point

APDU	Application protocol data unit
API	Access Point Identifier
ASE	Application service element
ASN.1	Abstract Syntax Notation One
CC	Connect confirm
CLNP	Connectionless network layer protocol
CLNS	Connectionless network layer service
CLR	Clear
CMIP	Common management information protocol
CMISE	Common management information service element
CONP	Connection oriented network-layer protocol
CP	Connection Point
CR	Connection request
CSES	Consecutive severely errored seconds
CV	Code violation
DCC	Data communications channel
DCN	Data communications network
DEG	Degraded signal
DS	Defect Second
EB	Errored Block
EBC	Errored Block Count
ECC	Embedded control channel
ES	Errored second
ESA	Errored Seconds Type A
ESB	Errored Seconds Type B
EXC	Excessive errors
EXER	Exercise
ExTI	Expected Trace Identifier
FBBE	Far-end Background Block Error
FC	Failure Counts
FDS	Far-end Defect Second
FEBC	Far-end Errored Block Count
FEBE	Far end block error
FES	Far-end Errored Second
FLS	Frame loss second
FOP	Failure of Protocol
FPME	Far-end Performance Monitoring Event

FSES	Far-end Severely Errored Second
FSw	Forced Switch
FU	Functional unit
GNE	Gateway network element
HO	Hold Off
IFU	Interworking functional unit
IP	Interworking protocol
IS	Intermediate system
ISO	International Organization for Standardization
LCN	Local communications network
LO	Lockout of protection
LOF	Loss of Frame
LOM	Loss of Multiframe
LOP	Loss of Pointer
LOS	Loss of Signal
LOW	Lockout of Working
LTC	Loss of Tandem Connection
MAF	Management applications function
MAINTREG	Maintenance Registers
MCF	Message communications function
MD	Mediation device
MF	Mediation function
MI	Management Information
MO	Managed object
MOC	Managed object class
MP	Management Point
MSw	Manual Switch
NBBE	Near-end Background Block Error
NDS	Near-end Defect Second
NE	Network element
NEBC	Near-end Errored Block Count
NEF	Network element function
NES	Near-end Errored Second
NLR	Network layer relay
NNE	Non-SDH network element
NPDU	Network protocol data unit
NPME	Near-end Performance Monitoring Event

NSAP	Network service access point
NSES	Near-end Severely Errored Second
OAM&P	Operations, administration, maintenance and provisioning
ODI	Outgoing Defect Indication
OEI	Outgoing Error Indication
OS	Operations system
OSF	Operations system function
OSI	Open systems interconnection
P	Protection
PDU	Protocol data unit
PERFREG	Performance Registers
PJC	Pointer Justification Count
PJE	Pointer justification event
PLM	Payload Mismatch
PPDU	Presentation protocol data unit
PSN	Packet switched network
QoS	Quality of service
RDI	Remote Defect Indication
REI	Remote Error Indication
ROSE	Remote operations service element
RTR	Reset Threshold Report
SAPI	Service access point identifier
SD	Signal Degrade
SDH	Synchronous digital hierarchy
SF	Signal Fail
SMN	SDH management network
SMS	SDH management subnetwork
SNDCF	Subnetwork dependent convergence function
SPDU	Session protocol data unit
SSF	Server Signal Fail
STM	Synchronous transport module
SVC	Switched virtual circuit
TCP	Termination Connection Point
TEI	Terminal end-point identifier
TIM	Trace Identifier Mismatch
TMN	Telecommunications management network
TP	Termination Point

TPDU	Transport protocol data unit
TR	Threshold Report
TSAP	Transport service access point
TSF	Trail Signal Fail
TSN	Time Slot Number
TxTI	Transmitted Trace Identifier
UAS	Unavailable second
UAT	Unavailable time
UI	Unnumbered information
UITS	Unacknowledged information transfer service
W	Working
WTR	Wait to Restore

5 SDH management network

5.1 Management network organizational model

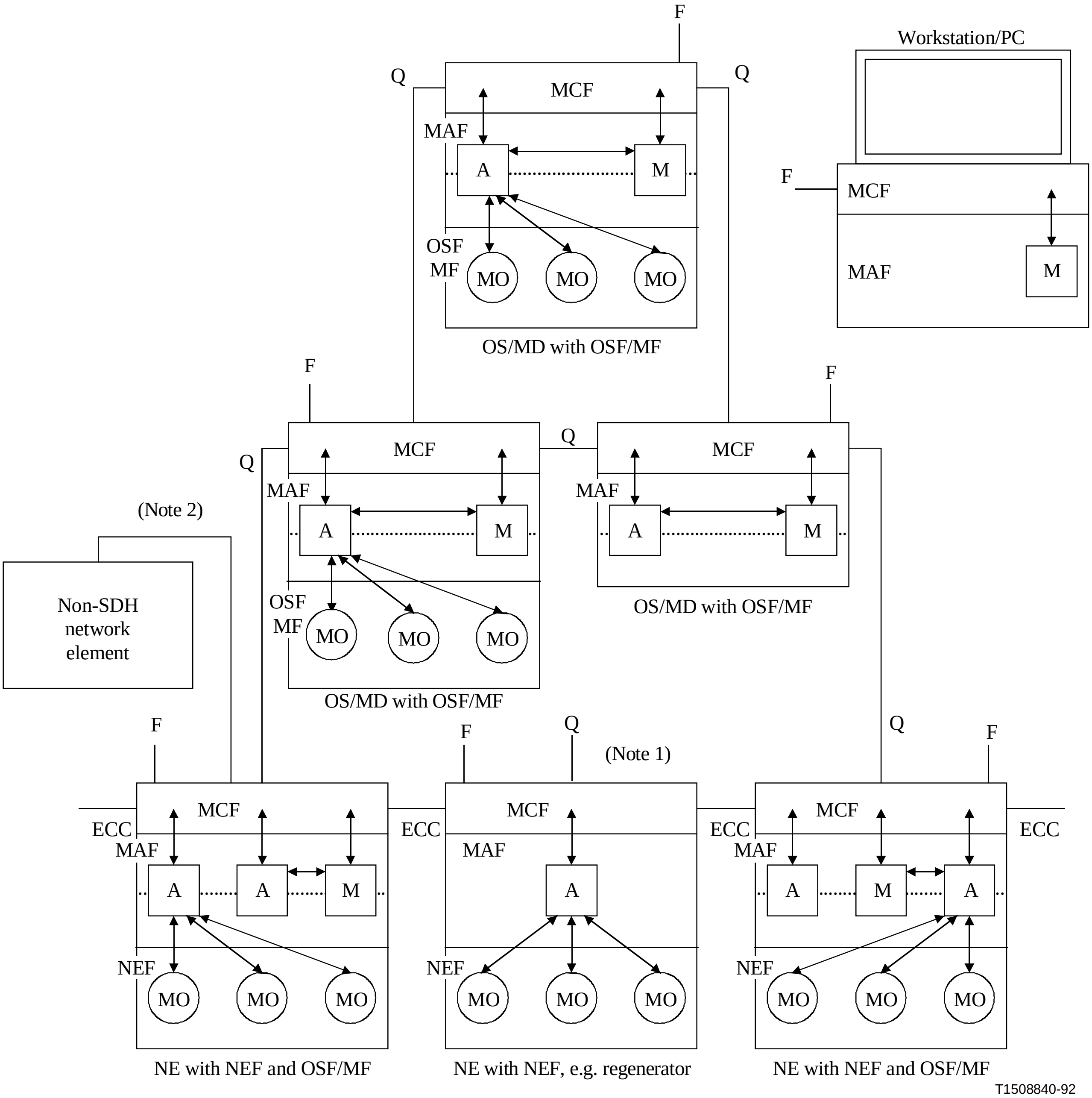
The management of an SDH network uses a multi-tiered distributed management process. Each tier provides a predefined level of network management capabilities. The lower tier of this organizational model (see Figure 5-1) includes the SDH NEs providing transport services. The management applications function (MAF) within the NEs communicates with, and provides management support to, peer NEs and mediation device(s) (MDs)/operations system(s) (OSs).

The communication process is provided via the message communications function (MCF) within each entity.

The MAF at each entity can include agents only, managers only, or both agents and managers. Entities that include managers are capable of managing other entities.

Each tier in the multi-tiered organizational model can provide additional management functionality. However, the message structure should remain the same. A manager within an SDH NE may suppress alarms generated by one or more of its managed NEs due to a common failure, and replace them by a new alarm message, directed to the OS/MD, identifying the source of the problem. The new alarm message format will be consistent with other alarm messages.

The message format will be maintained as messages are elevated up the hierarchy, i.e. SDH NE to SDH NE messages will have the same structure as SDH NE to MD messages and SDH MD to OS messages.



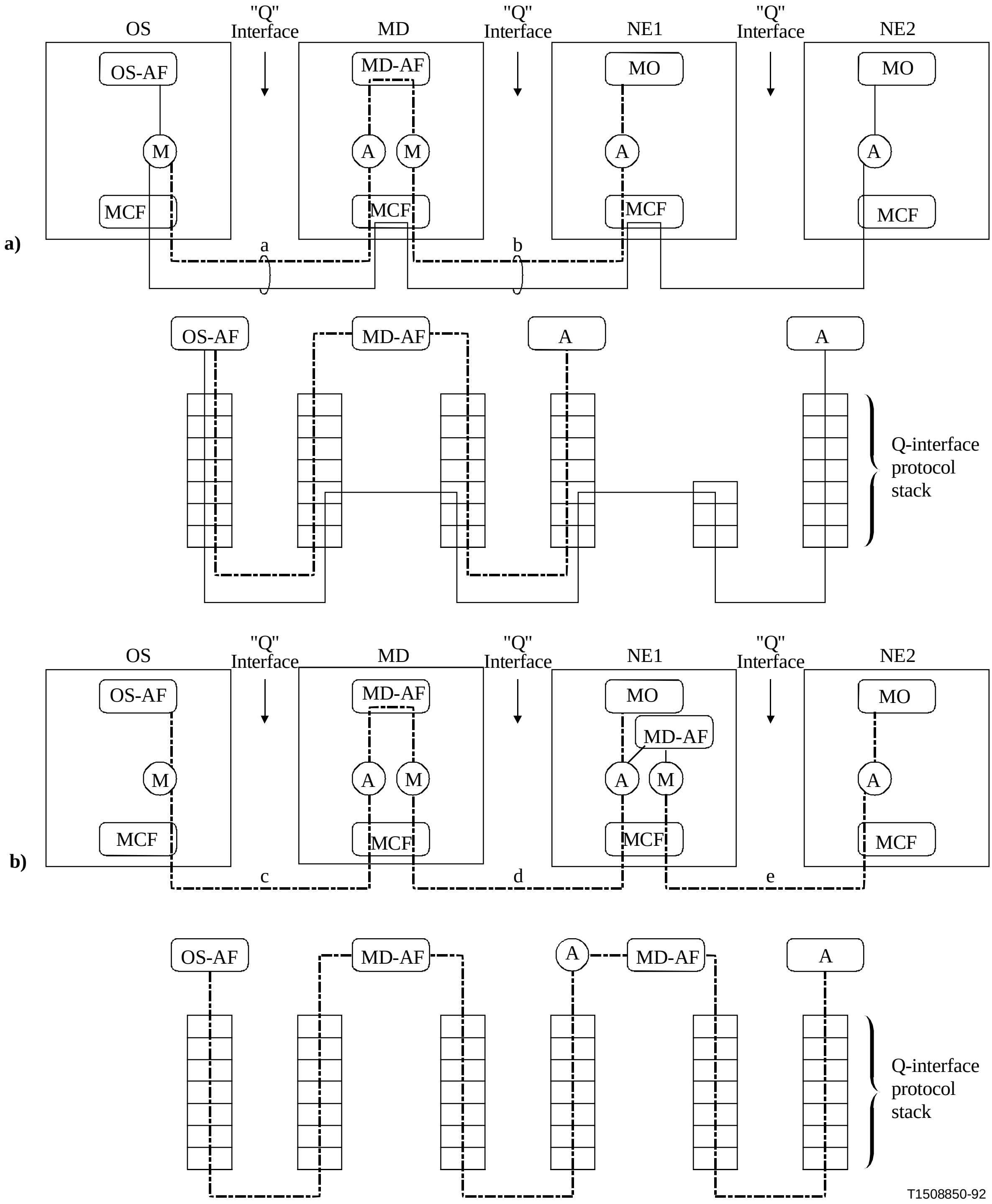
MCF	Message communications function
MAF	Management applications function
NEF	Network element function
ECC	Embedded control channel
A	Agent
M	Manager
MO	Managed object

NOTE 1 – Use of this interface may be foreseen in some applications.

NOTE 2 – For further study.

NOTE 3 – The designation "Q" is used in a generic sense.

Figure 5-1/G.784 – Management organizational model



OS	Operations system
MD	Mediation device
NE	Network element
OS-AF	OS-application function
MD-AF	MD-application function
MCF	Message communications function
A	Agent
M	Manager
MO	Managed object

Figure 5-2/G.784 – SDH management examples

Figure 5-2 a) illustrates examples of management communication using a Q-interface implemented in the MCF where logically independent communications are provided over a single physical interface:

– between a manager in the OS and two different agents; one in the MD and one in NE2 (interface a);

– between a manager in the MD and an agent in NE1; between a manager in the OS and an agent in NE2 (interface b).

Figure 5-2 b) illustrates examples of management communication using Q-interface protocols implemented in the MCF:

– between a manager in the OS and an agent in the MD (interface c);

– between a manager in the MD and an agent in NE1 (interface d);

– between a manager in NE1 and an agent in NE2 (interface e).

5.2 Relationship between SMN, SMS and TMN

The inter-relationship between the SMN, SMS and TMN is shown in Figure 5-3. Figure 5-4 shows specific examples of SMN, SMSs and connectivities within the encompassing TMN.

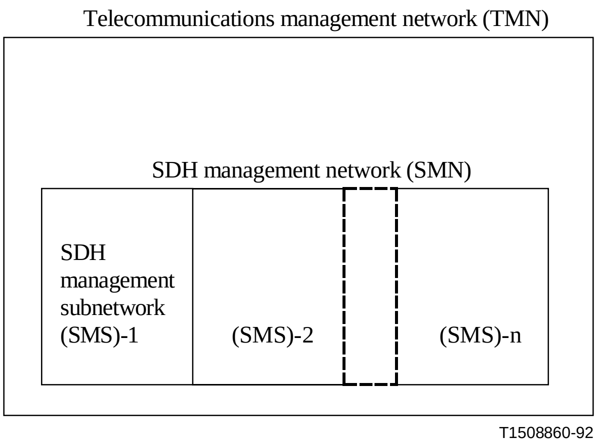
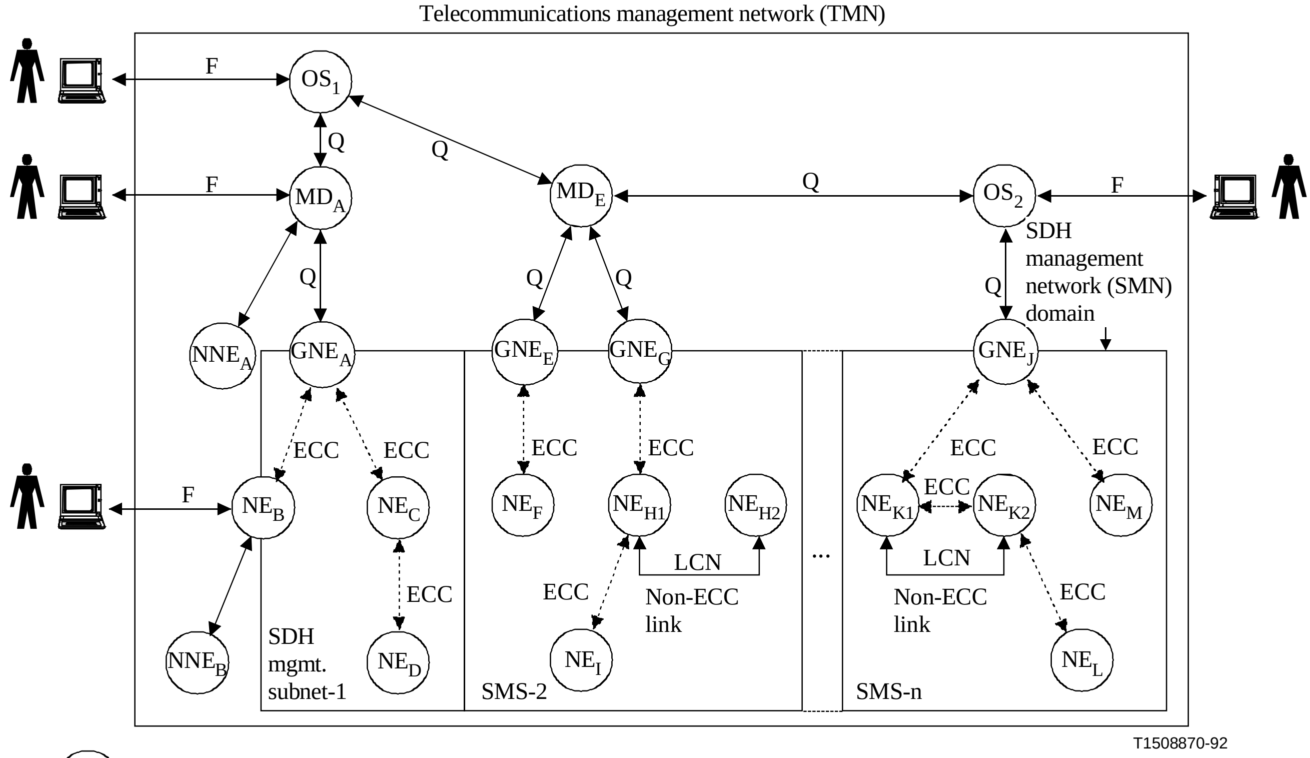


Figure 5-3/G.784 – Relationship between SMN, SMS and TMN



Communications blocks (OS, MD, GNE, NE)

Communications links using standard Q-interface protocol

SDH ECC

LCN Local communications network

GNE Gateway network element (see 5.3.1)

NOTE – The designation "Q" is used in a generic sense.

Figure 5-4/G.784 – TMN, SMN, SMS model

The following subclauses describe the SMS in more detail, addressing:

– access to the SMS; and

– SMS architecture.

5.2.1 Access to the SMS

Access to the SMS is always by means of an SDH NE functional block. The SDH NE may be connected to other parts of the TMN through the following sets of interfaces:

1) workstation (F);
2) mediation device (a Q-interface);
3) operations system (a Q-interface);
4) non-SDH NE or site related information [interface(s) for further study].

The functionality required to be supported by the SDH NE will determine the type of Q-interface to be provided. For instance, the two main varieties of SDH NEs expected are the SDH NEs with mediation functions (MF) and "regular" SDH NEs. An example of the SDH NE with MF is shown in Figure 5-5. An example of a "regular" SDH NE is shown in Figure 5-6.

5.2.2 SDH management subnetwork architecture

In Figure 5-4, a number of points should be noted concerning the architecture of the SMS:

a) *Multiple NEs at a single site*

Multiple, addressable SDH NEs may appear at a given site. For example, in Figure 5-4 NE_E and NE_G may be collocated at a single equipment site.

b) *SDH NEs and their communications functions*

The message communications function of an SDH NE terminates (in the sense of the lower protocol layers), routes or otherwise processes messages on the ECC, or connected via an external Q-interface.

i) All NEs are required to terminate the ECC. In OSI terms, this means that each NE must be able to perform the functions of an end system.

ii) NEs may also be required to route ECC messages between ports according to routing control information held in the NE. In OSI terms, this means that some NEs may be required to perform the functions of an intermediate system.

iii) NEs may also be required to support Q- and F-interfaces.

c) *SDH inter-site communications*

The inter-site or inter-office communications link between SDH NEs will normally be formed from the SDH ECCs.

d) *SDH intra-site communications*

Within a particular site, SDH NEs may communicate via an intra-site ECC or via an LCN. Figure 5-4 illustrates both instances of this interface.

NOTE – A standardized LCN for communicating between collocated network elements has been proposed as an alternative to the use of an ECC. The LCN would potentially be used as a general site communications network serving both SDH and non-SDH NEs (NNEs). The LCN is part of the TMN and thus the specification of the LCN is beyond the scope of this Recommendation.

5.3 SMS topology and reference models

5.3.1 ECC topology for the SDH management subnetwork

It is intended that this Recommendation should place no restriction on the physical transport topology to support the ECC. Thus it is expected that the supporting DCCs may be connected using string (bus), star, ring or mesh topologies.

Each SDH management subnetwork (SMS) must have at least one element which is connected to an OS/MD. This is called a gateway network element (GNE) and is illustrated in Figures 5-5, 5-6 and 5-7. The GNE should be able to perform an intermediate system network layer routing function for ECC messages destined for any end system in the SMS.

NOTE – This is a specific instance of the general requirement that messages passing between communicating subnetworks shall use the network layer relay.

The communications function is illustrated in Figure 5-7. Messages passing between OS/MD and any of the end systems in the subnetwork are routed through the GNE and, in general, other intermediate systems.

5.3.2 Message routing at SDH NE sites

The means of generation and administration of routing control information amongst communicating subnetworks and within subnetworks is detailed in 8.2.3.

5.3.3 SMS reference models

Reference models are particularly suited for test cases and for design verification and acceptance testing. The reference configurations in Figures 5-8 and 5-9 are examples of test cases for SMS management. Examples of SMS connectivity are given in Figure 5-10.

Other variations of Figure 5-9 are also of interest as reference configurations; for example, on routes where the operator chooses not to implement the multiplex section protection (MSP) function, the ECCs would be provided on at least two SDH lines, and optionally on any remaining SDH lines of a particular route.

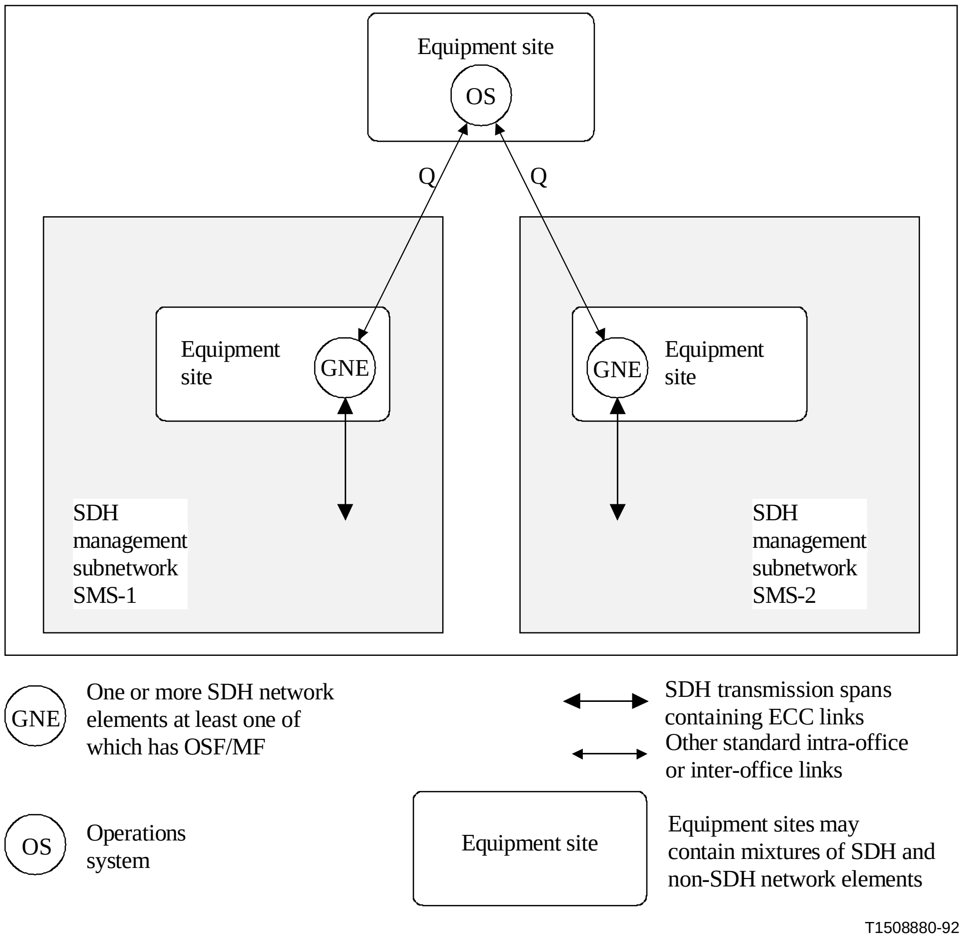


Figure 5-5/G.784 – SDH ECC topology for sites containing SDH NE with OSF/MF functionality

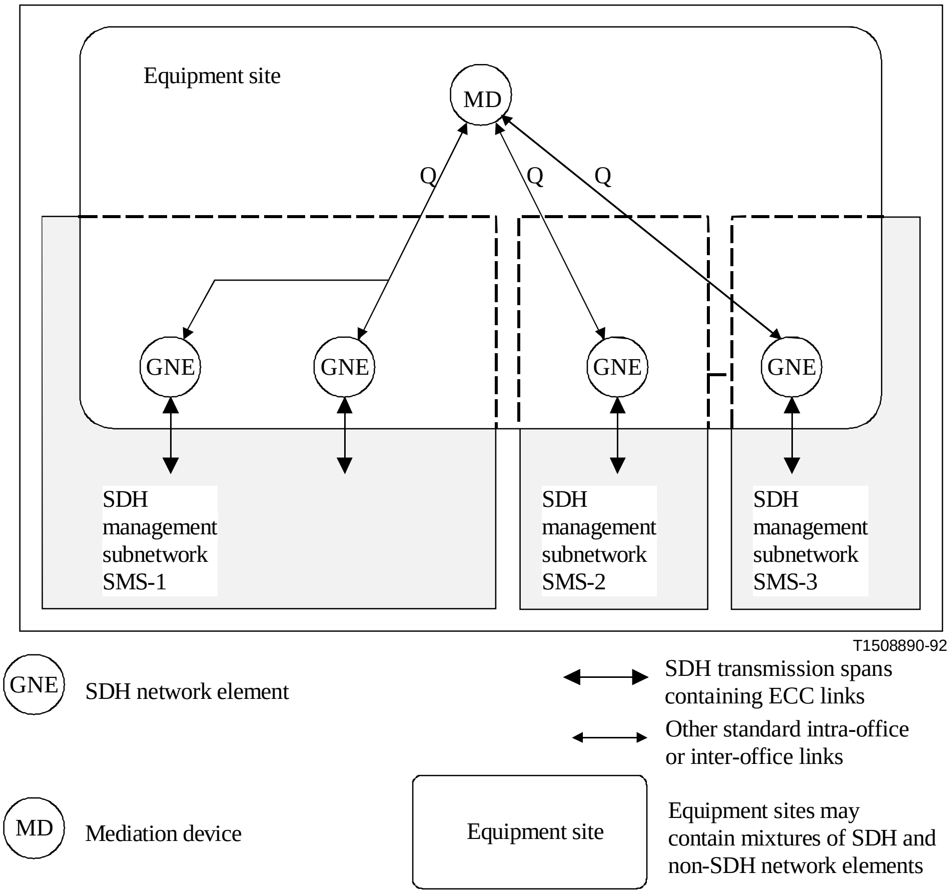
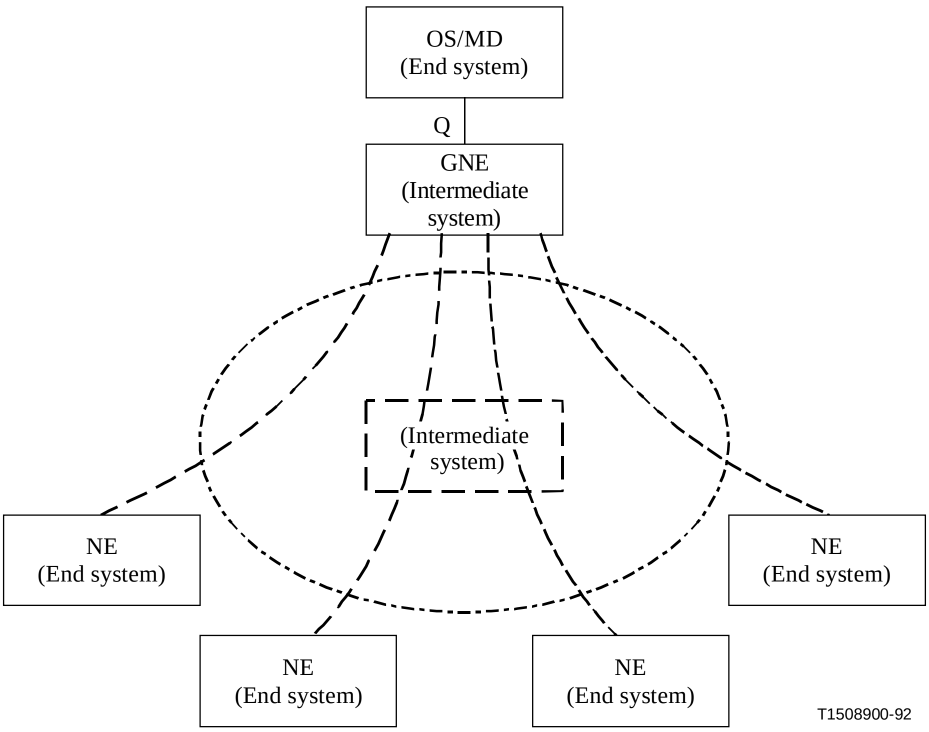
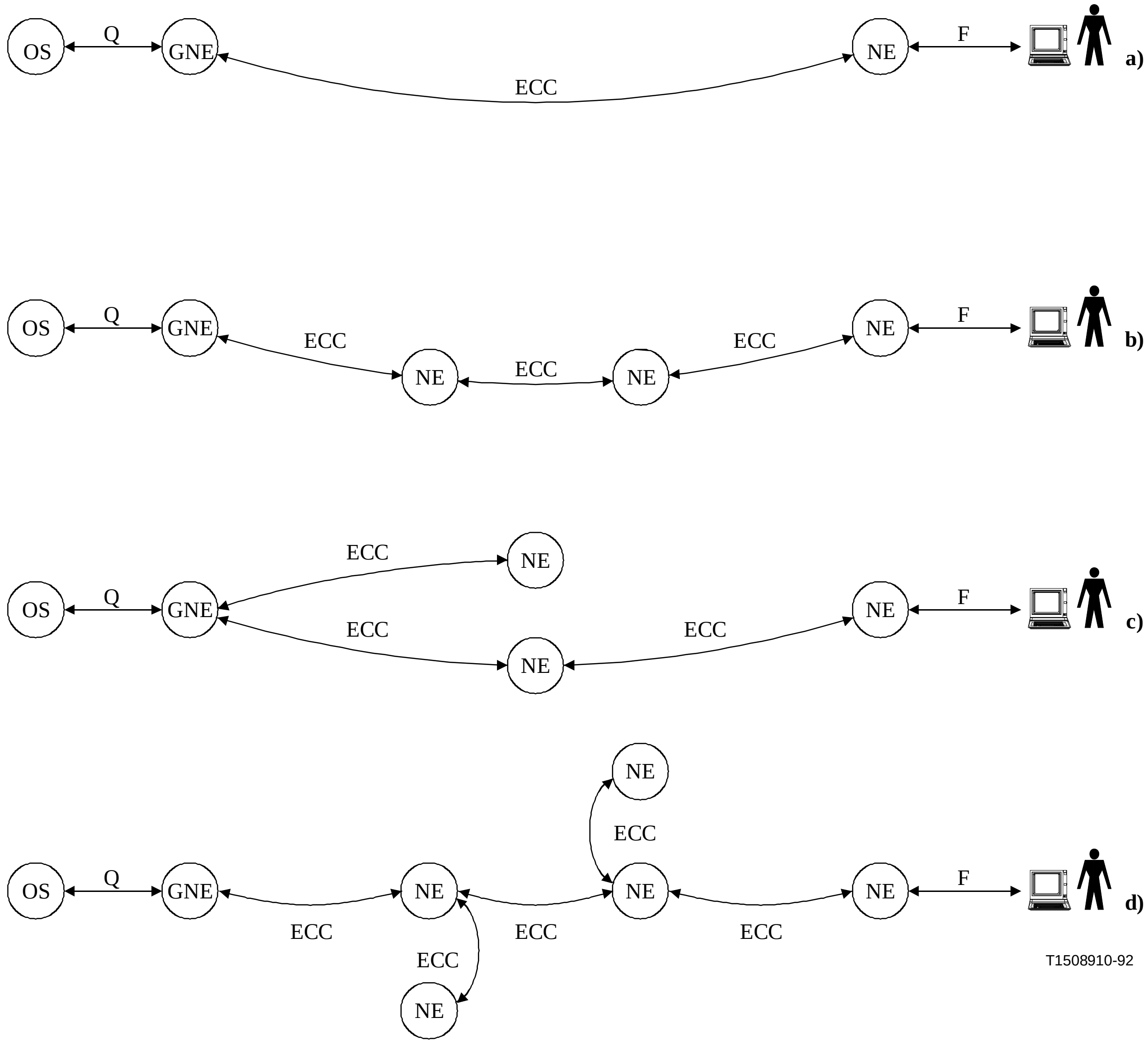


Figure 5-6/G.784 – SDH ECC topology for sites with mediation devices



GNE Gateway network element

Figure 5-7/G.784 – The concept of intermediate and end systems



GNE Gateway network element
NE Network element

NOTE – The ECCs are assumed to be protected by a 1+1 protection system whenever possible.

Figure 5-8/G.784 – Reference models for ECC configuration

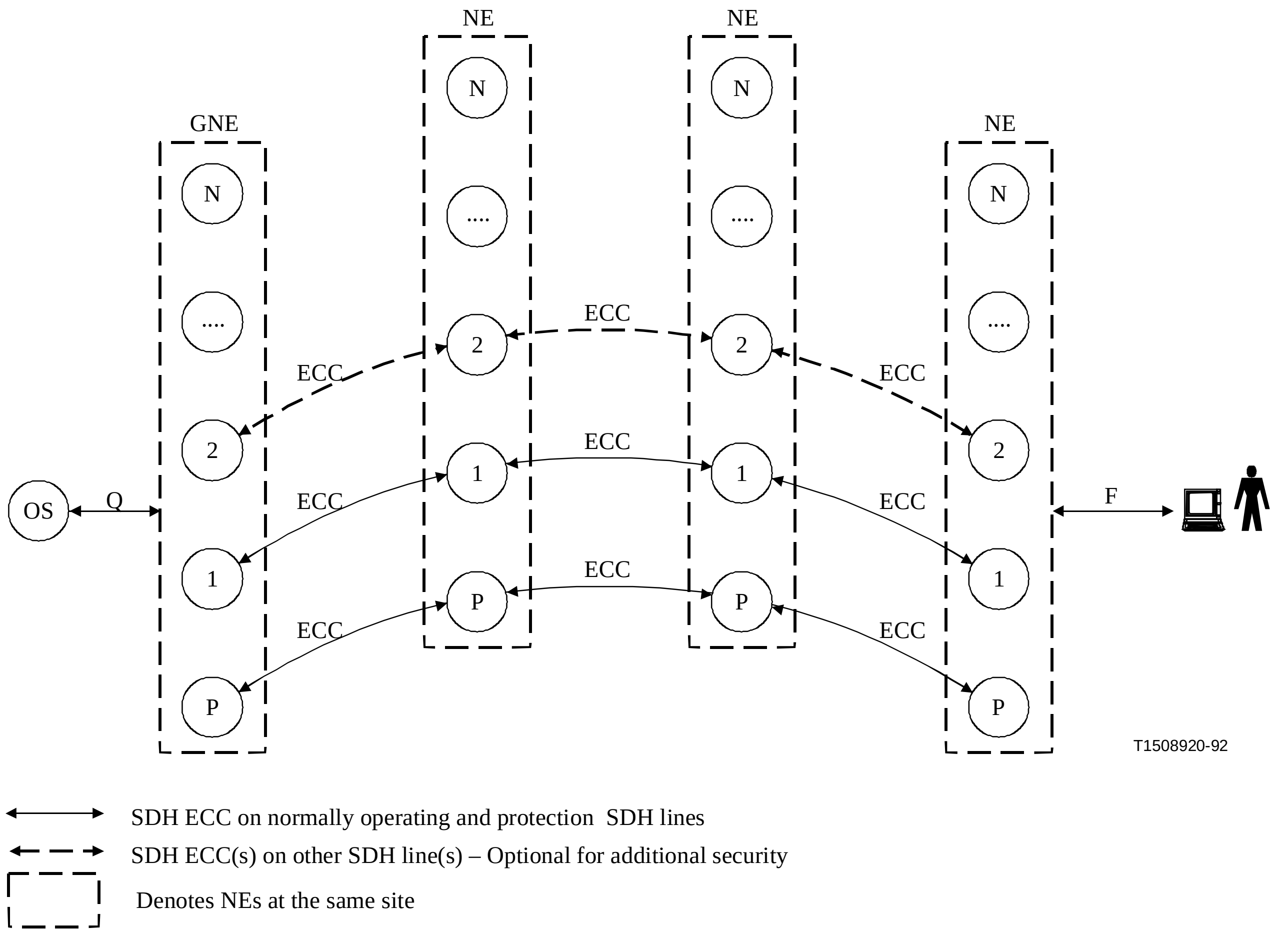


Figure 5-9/G.784 – Reference models showing the provision of 1+1 protected ECC on a 1:n SDH line system

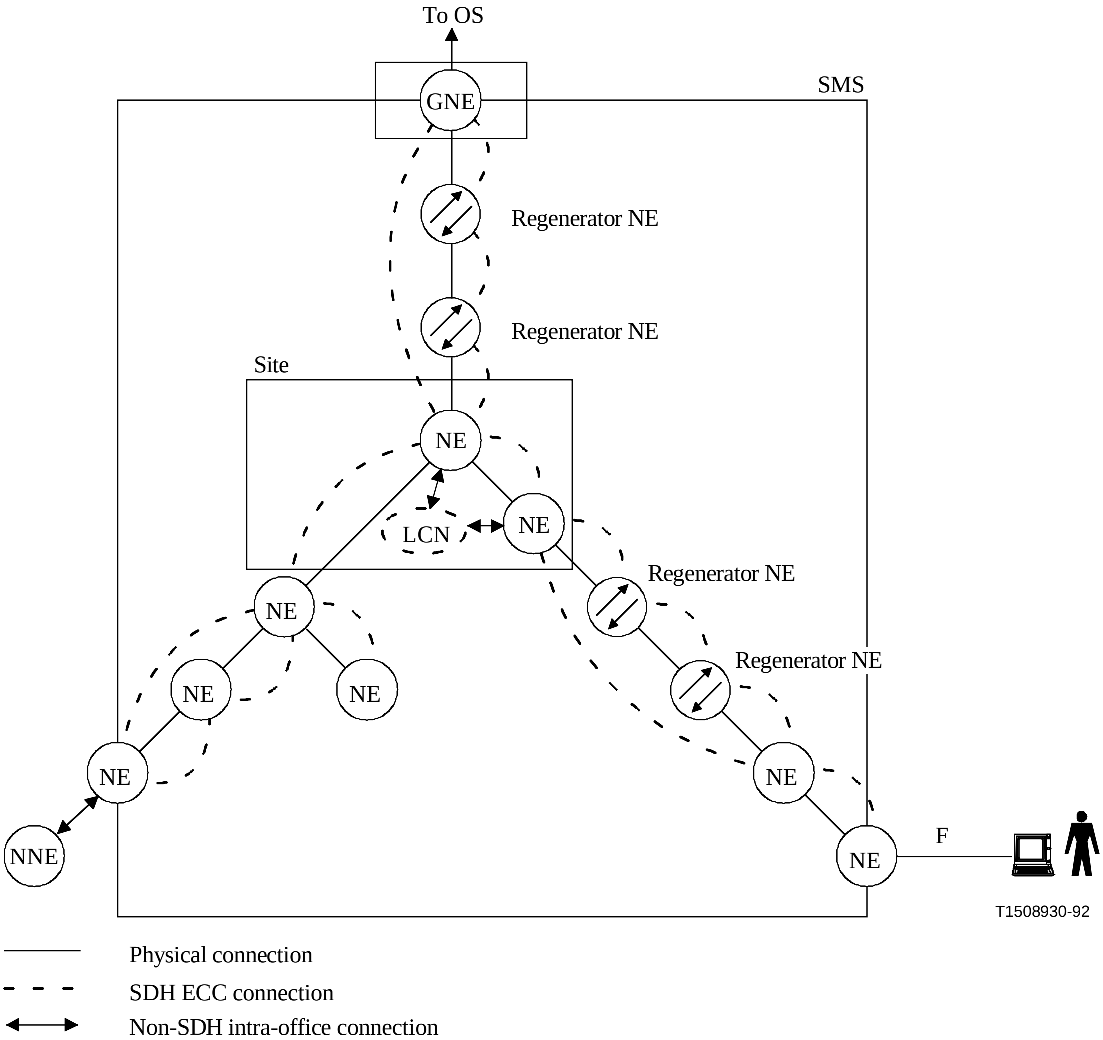


Figure 5-10/G.784 – Examples of SMS connectivity

6 Information model

The information model is defined in Recommendation G.774 [12] and G.774.x-series Recommendations.

7 Management functions

This clause provides an overview of the minimum functions which are required to support inter-vendor/network communications and single-ended maintenance of SDH NEs within an SMS, or between communicating peer NEs across a network interface (see 7.1.1, 7.2.1, 7.3.1, 7.4.2). Single-ended maintenance is the ability to access remotely located NEs to perform maintenance functions.

Other management functions have been identified (see 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.2.4, 7.2.5, 7.4.1, 7.4.3, 7.5). They are for further study.

It should be noted that the management functions have been categorized according to the classifications given in Recommendation M.3000.

Detailed specifications of the management functions, in terms of managed objects classes, attributes and message specification, are given in the G.774-series Recommendations.

SEMF overview

The (synchronous) equipment management function [(S)EMF] (see Figure 7-1) provides the means through which the synchronous network element function (NEF) is managed by an internal or external manager. If a network element (NE) contains an internal manager, this manager will be part of the SEMF.

The SEMF interacts with the other atomic functions (refer to Recommendation G.783) by exchanging information across the MP reference points. The SEMF contains a number of filters that provide a data reduction mechanism on the information received across the MP reference points. The filter outputs are available to the agent via the network element resources and management applications functions (MAF) which represent this information as managed objects.

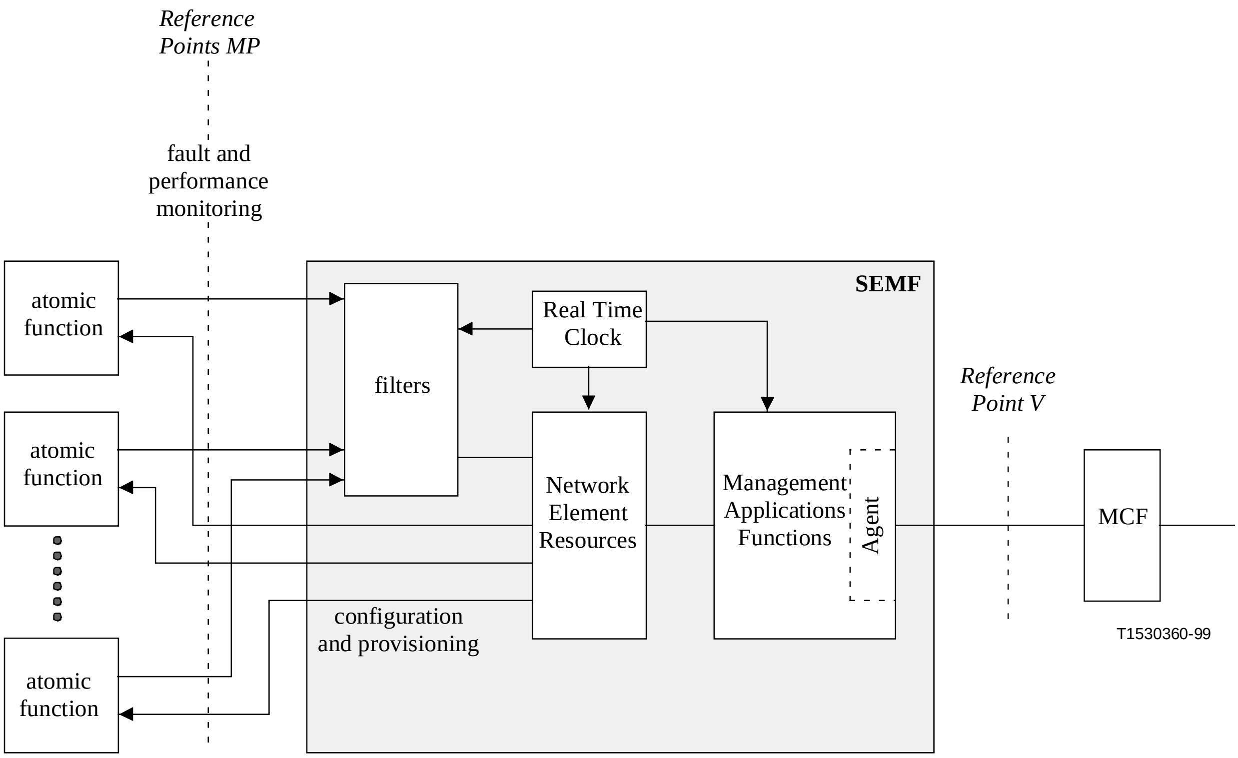


Figure 7-1/G.784 – Synchronous Equipment Management Function

Network element resources provide event processing and storage. The MAF processes the information provided to and by the NE resources. The agent converts this information to CMISE (common management information service element) messages and responds to CMISE messages from the manager by performing the appropriate operations on the managed objects.

This information to and from the agent is passed across the V reference point to the message communications function (MCF).

Supervision processes

Figure 7-2 shows a high level view of the supervision process within a network element. The subprocesses at the left side in Figure 7-2 are performed in atomic functions (refer to Recommendation G.783), while the other subprocesses are performed in the (synchronous) equipment management function [(S)EMF] described in 7.2 (fault management) and 7.3 (performance monitoring). These latter ones represent the filters in Figure 7-1.

The interface between the processing in the atomic functions and the equipment management function is indicated by the dashed line in Figure 7-2. It represents the MP reference points as defined in Recommendation G.783. For performance monitoring, the signals passed over this interface are the 1 second signals pXXX [XXX is e.g. Near-end Errored Block Counts (N_EBC), Far-end Defect Seconds (F_DS), positive Pointer Justification Counts (PJC+)]. For fault management, the signals passed over this interface are the fault cause signals cXXX (XXX is e.g. LOS, TIM).

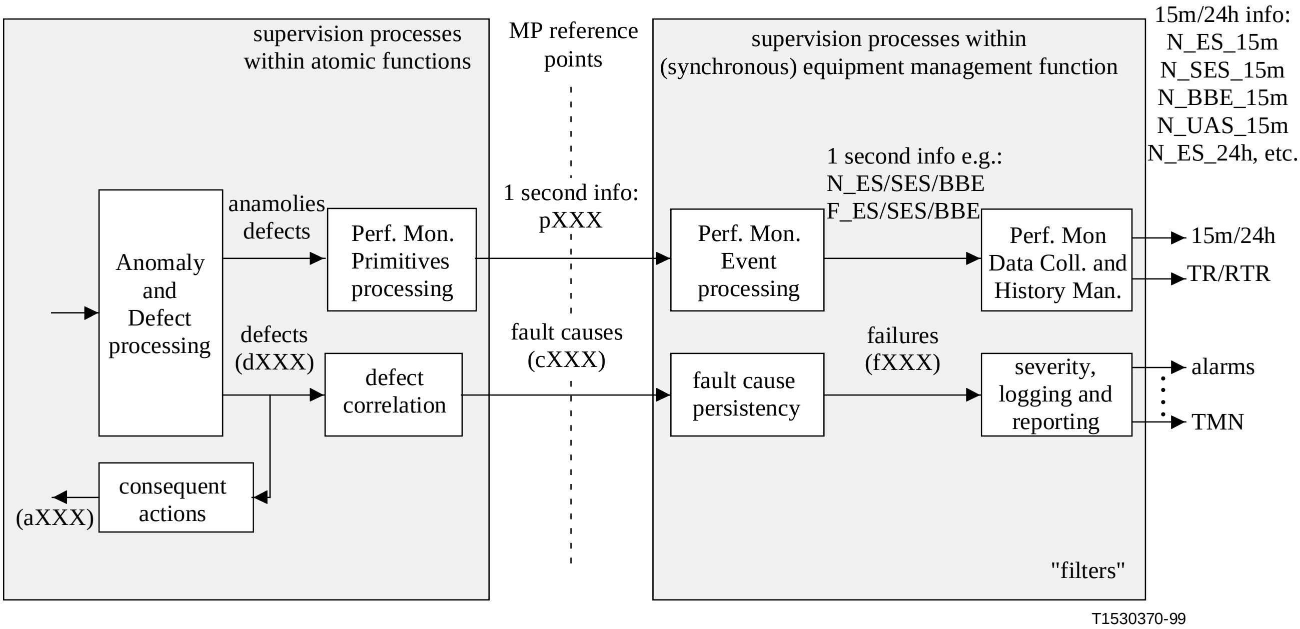


Figure 7-2/G.784 – Supervision process within (synchronous) equipment management function

The filtering functions (Figures 7-1, 7-2) provide a data reduction mechanism on the fault cause (cXXX) and performance monitoring primitives (pXXX) information presented at the MP reference points. Two types of techniques can be distinguished:

– The fault cause persistency filter will provide a persistency check on the fault causes that are reported across the MP reference points. In addition to the transmission failures listed above, hardware failures with signal transfer interruption are also reported at the input of the fault cause filter for further processing.

– The performance monitoring events processing processes the information available from the one second window (see Recommendation G.783) and reported across the MP reference points to derive e.g. errored seconds and severely errored seconds, background block errors, etc.

NOTE – One second filters in the atomic functions (see Recommendation G.783) perform a simple integration of reported anomalies by counting during a one second interval. In addition, defects are filtered by the one second filter. At the end of each one second interval the contents of the counters may be obtained by the SEMF.

Configuration and provisioning

Network elements may support several functions which can be operated only in exclusivity of each other. Examples are:

i) a 140/155 Mbit/s interface unit which can operate either in a 140 Mbit/s mode or a STM-1 mode;

ii) a 2 Mbit/s interface unit which allows mapping of the 2 Mbit/s into a VC-12 in either an asynchronous mapping mode or a byte synchronous mapping mode;

iii) establishment of a protection relation between two signals;

iv) establishment of a protection relation between two field replaceable units which can operate either as two unprotected units, or as one protected pair.

Besides such configuration provisionings, provisionings are needed for parameters in individual processes within a NE. Examples are: protection switching, trace identifier, matrix connection, error defect thresholds, Portmode and TPmode, reporting of consequential defects/failures (e.g. AIS, RDI, ODI).

Information flows over Management Points (MP)

The information flows described in this clause are functional. The existence of these information flows in the equipment will depend on the functionality provided by the NE and the options selected.

The information flow over the MP reference points that arises from anomalies and defects detected in the atomic functions is described in specific details for each atomic function in Recommendation G.783.

The information flow over the MP reference points that arises from configuration and provisioning data is described in specific details for each atomic function in Recommendation G.783. The information listed under Set refers to configuration and provisioning data that is passed from the SEMF to the atomic functions. The information listed under Get refers to status reports made in response to a request from the SEMF for such information.

As an example we may consider the higher order path trace. The higher order path termination may be provisioned for the HO path trace ID that it should expect by a "Set_Rx_HO_path_trace_ID" command received from the manager. If the HO path trace that is received does not match the expected HO path trace, this will give rise to a report of a mismatch of the HO path trace across the hp_nm reference point. Having received this mismatch indication, the NE stores it for access by the manager.

7.1 General functions

7.1.1 Embedded control channel (ECC) management

SDH NEs communicate via the ECC. In order to have the ECC network operate properly, a number of management functions are required. Examples are:

a) retrieval of network parameters to ensure compatible functioning, e.g. packet size, timeouts, quality of service, window size, etc.;

b) establishment of message routing between DCC nodes;

c) management of network addresses;

d) retrieval of operational status of the DCC at a given node; and

e) capability to enable/disable access to the DCC.

The definitions of these functions are for further study.

7.1.2 Security

For further study.

7.1.3 Software

For further study.

7.1.4 Remote log-in

For further study.

7.1.5 Time-stamping

Events, performance reports and registers containing event counts that require time-stamping shall be time stamped with a resolution of one second relative to the NE local real time clock. The required accuracy of the NE real time clock and precise details of the time-stamping of events/reports relative to UTC are for further study.

NOTE – A maximum value for the NE real time clock accuracy is considered to be in the range 1 to 10 s.

The start of 15-minute and 24-hour counts should be accurate to within ±10 s with respect to the NE real time clock. For example, a 15-minute register may begin its 2:00 count between 1:59:50 and 2:00:10[1].

7.2 Fault (maintenance) management

7.2.1 Fault cause persistency filter

The equipment management function within the network element performs a persistency check on the fault causes before it declares a fault cause a failure.

A transmission failure (fXXX) shall be declared if the fault cause persists continuously for 2.5 ± 0.5 s. The failure shall be cleared if the fault cause is absent continuously for 10 ± 0.5 s.

Transmission failures associated with the three types (termination, adaptation, connection) of transport atomic functions are listed in Table 7-1. The specific set of failures associated with each atomic function are to be derived from the specific set of fault causes defined in the atomic function.

NOTE – A complementary list is available in Recommendation M.3100.

The failure declaration and clearing shall be time stamped. The time-stamp shall indicate the time at which the fault cause is activated at the input of the fault cause persistency (i.e. defect-to-failure integration) filter, and the time at which the fault cause is deactivated at the input of the fault cause persistency filter.

---

[1] These values may be reviewed during the next study period.

Table 7-1/G.784 – Atomic function associated failure list

Termination sink	Adaptation sink	Connection
fUNEQ (unequipped)	fLOF (loss of frame)	fFOP (failure of protocol)
fTIM (trace identifier mismatch)	fLOM (loss of multiframe)	
fEXC (excessive errors)	fLOP (loss of pointer)	
fDEG (degraded)	fAIS (alarm indication signal)	
fLOS (loss of signal)	fPLM (payload mismatch)	
fRDI (Note) (remote defect indication)		
fODI (outgoing defect indication)		
fLTC (loss of tandem connection)		
fAIS (alarm indication signal)		
NOTE – When using the enhanced-RDI option described in Appendix VII/G.707, additional RDI failures will exist.		

7.2.2 Alarm surveillance

Alarm surveillance is concerned with the detection and reporting of relevant events and conditions which occur in the network. In a network, events and conditions detected within the equipment and incoming signals should be reportable. In addition, a number of events external to the equipment should also be reportable. Alarms are indications that are automatically generated by an NE as a result of the declaration of a failure. The OS shall have the ability to define which events and conditions generate autonomous reports, and which shall be reported on request.

The following alarm-related functions shall be supported:

– autonomous reporting of alarms;

– request for reporting of all alarms;

– reporting of all alarms;

– allow or inhibit of autonomous alarm reporting;

– reporting on request status of allow or inhibit alarm reporting;

– enabling and disabling (via MI_XXX_Reported) of the declaration of AIS, RDI and ODI fault causes in the atomic functions. Refer to 2.2.4/G.783;

– control of the termination point mode of termination points. Refer to 2.2.1/G.783.

– optionally, control of the port mode of termination points. Refer to 2.2.1/G.783.

– reporting of protection switch events.

7.2.3 Alarm history management

Alarm history management is concerned with the recording of alarms. Historical data shall be stored in registers in the NE. Each register contains all the parameters of an alarm message.

Registers shall be readable on demand or periodically. The OS can define the operating mode of the registers as wrapping or stop when full. The OS may also flush the registers or stop recording at any time.

NOTE – Wrapping is the deletion of the earliest record to allow a new record when a register is full. Flushing is the removal of all records in the register.

7.2.4 Testing

For further study.

7.2.5 External events

For further study.

7.3 Performance monitoring

NOTE – This subclause defines the performance monitoring related equipment specifications based on the network level specifications in Recommendations M.2100, M.2101.1, M.2120, G.826 and G.827.

Performance monitoring is a process consisting of performance monitoring event processes and performance monitoring data collection and history processes.

Within performance monitoring the concepts of "near-end" and "far-end" are used to refer to performance monitoring information associated with the two directions of transport of a bidirectional trail. For a bidirectional trail from A to Z:

– at node A the near-end information represents the performance of the unidirectional trail from Z to A, while the far-end information represents the performance of the unidirectional trail from A to Z;

– at node Z the near-end information represents the performance of the unidirectional trail from A to Z, while the far-end information represents the performance of the unidirectional trail from Z to A;

– at an intermediate node I in the unidirectional trail A to Z the near-end information represents the performance of the unidirectional trail segment from A to I, while the far-end information represents the performance of the unidirectional trail from Z to A;

– at an intermediate node I in the unidirectional trail Z to A the near-end information represents the performance of the unidirectional trail segment from Z to I, while the far-end information represents the performance of the unidirectional trail from A to Z.

At either end of the trail (A or Z), the combination of near-end and far-end information present the performance of the two directions of the trail.

At an intermediate node in the trail (I), the combination of far-end information in the trail signal from A to Z and far-end information in the trail signal from Z to A present the performance of the two directions of the trail.

See Appendix I.

7.3.1 Performance monitoring event process

The performance monitoring event processing processes the information available from the performance monitoring primitives processing (atomic functions, G.783) giving the performance primitives (EBC and DS) to derive the performance events (e.g. errored seconds, severely errored seconds and background block errors)[2].

Figure 7-3 presents the processes and their interconnect within the Near-end Performance Monitoring Event (NPME) function.

NES process: A Near-end Errored Second (NES) shall be generated if the defect second (NDS) is set or if the near-end errored block count (NEBC) is greater or equal to 1: NES(t) ← (NDS = true) or (NEBC ≥ 1).

NSES process: A Near-end Severely Errored Second (NSES) shall be generated if the near-end defect second (NDS) is set or if the near-end errored block count (NEBC) is greater or equal to 30% (path level), 15% (STM-1 multiplex section level) of the blocks in a one second period: NSES(t) ← (NDS = true) or (NEBC ≥ "30% [15%] of blocks in a one second period").

NOTE 1 – It may be necessary to have a (fixed) SES threshold different from 30% Errored Blocks in section layers.

NBBE process: The number of near-end background block errors (NBBE) in a one second period shall be equal to the near-end errored block count (NEBC) if the second is not a near-end severely errored second (NSES). Otherwise (NSES is set), NBBE shall be zero. NBBE(t) ← NEBC (NSES = false) or 0 (NSES = true).

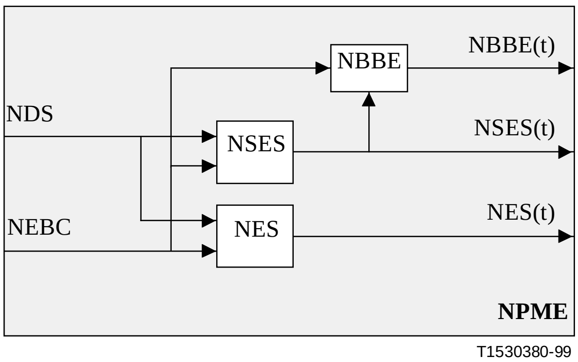


Figure 7-3/G.784 – Near-end performance monitoring event (NPME) function

Figure 7-4 presents the processes and their interconnect within the Far-end Performance Monitoring Event (FPME) function.

NOTE 2 – Far-end represents either those signals that are called "far-end" or "remote" or those signals that are called "outgoing". The latter is tandem connection specific.

FES process: A far-end Errored Second (FES) shall be generated if the defect second (FDS) is set or if the far-end errored block count (FEBC) is greater or equal to 1, and if that second is not a Near-end Defect Second (NDS): FES(t) ←(NDS = false) and [(FDS = true) or (FEBC ≥ 1)].

---

[2] The defects giving rise to an (S)ES are listed generically in Annex C/G.826, and specifically in each atomic function in Recommendation G.783.

FSES process: A far-end Severely Errored Second (FSES) shall be generated if the far-end defect second (FDS) is set or if the far-end errored block count (FEBC) is greater or equal to 30% (path level), 15% (STM-1 multiplex section level) of the blocks in a one second period, and that second is not a near-end defect second (NDS): FSES(t) ← (NDS = false) and [(FDS = true) or (FEBC ≥ "30% [15%] of blocks in a one second period")].

NOTE 3 – It may be necessary to have a (fixed) SES threshold different from 30% Errored Blocks in section layers.

FBBE process: The number of far-end background block errors (FBBE) in a one second period shall be equal to the far-end errored block count (FEBC) if the second is not a far-end severely errored second (FSES), and if that second is not a Near-end Defect Second (NDS). Otherwise (FSES is set), FBBE shall be zero. FBBE(t) ← FEBC (FSES = false and NDS = false) or 0 (FSES = true or NDS = true).

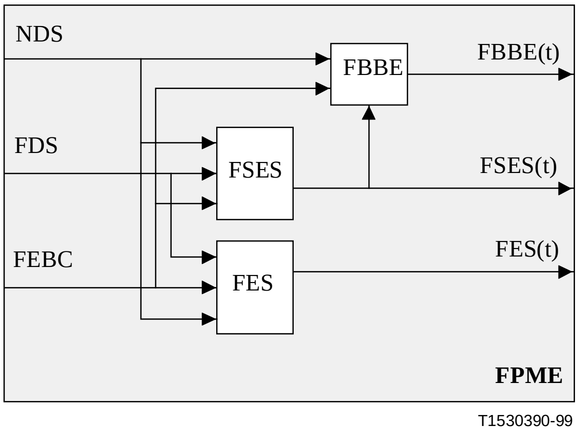


Figure 7-4/G.784 – Far-end performance monitoring event (FPME) function

7.3.2 Performance data collection

Performance data collection refers to the event counting associated with each of the performance events BBE, ES, SES as defined in Recommendation G.826, and any additional performance parameter defined in this Recommendation.

Two types of performance data collection are defined:

– the collection as specified in Recommendation M.2120, i.e. based on information of each direction of transport independently. This type is further referred to as performance data collection for maintenance purposes.

– the collection as specified in Recommendation G.826, i.e. based on information of both directions of transport together. This type is further referred to as performance data collection for error performance assessment purposes.

7.3.2.1 Performance data collection for maintenance purposes

This type of collection counts the events over fixed time periods of 15 minutes and 24 hours (Figures 7-5a, 7-5b, 7-5c). Counting is stopped during unavailable time (see 7.3.3).

These counters operate as follows:

15-minute counter

The performance events (e.g. SES) are counted in a counter per event (Figures 7-5b, 7-5c). These counters are called the current registers.

At the end of the 15-minute period the contents of the current registers are transferred to the first of the recent registers (see 7.3.4), with a time-stamp to identify the 15-minute period (including the day), after which the current register shall be reset to zero. It is an option not to transfer the content of a current register to a recent register if this content is zero[3].

It shall be possible to reset an individual current register to zero by means of an external command. The modularity of this command shall be as specified in Recommendation G.774.1.

Any register the content of which is suspect shall be flagged, using the "suspect interval flag" provided in Recommendation Q.822. This flag shall be raised independently for far-end and near-end counts. Examples of conditions to raise this flag are provided in Recommendation Q.822.

24-hour counter

The performance events (e.g. SES) are counted in a counter per event, independent of the 15-minute counters (Figures 7-5b, 7-5c). These counters are called the current registers. It was agreed that it is up to the NE implementation to update the register counts. It is not required that it be done on a second by second basis.

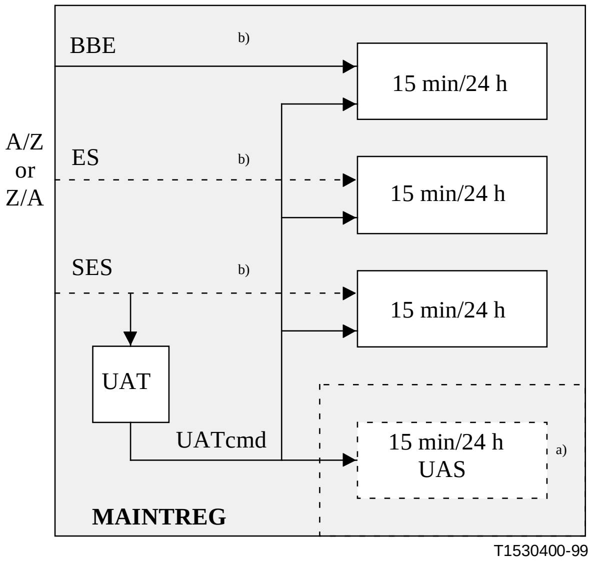
At the end of the 24-hour period the contents of the current registers are transferred to recent registers (see 7.3.4), with a time-stamp to identify the 24-hour period, after which the current register shall be reset to zero.

It shall be possible to reset an individual current register to zero by means of an external command. The modularity of this command shall be as specified in Recommendations G.774.1 and G.774.6.

Any register the content of which is suspect shall be flagged, using the "suspect interval flag" provided in Recommendation Q.822. This flag shall be raised independently for far-end and near-end counts. Examples of conditions to raise this flag are provided in Recommendation Q.822.

---

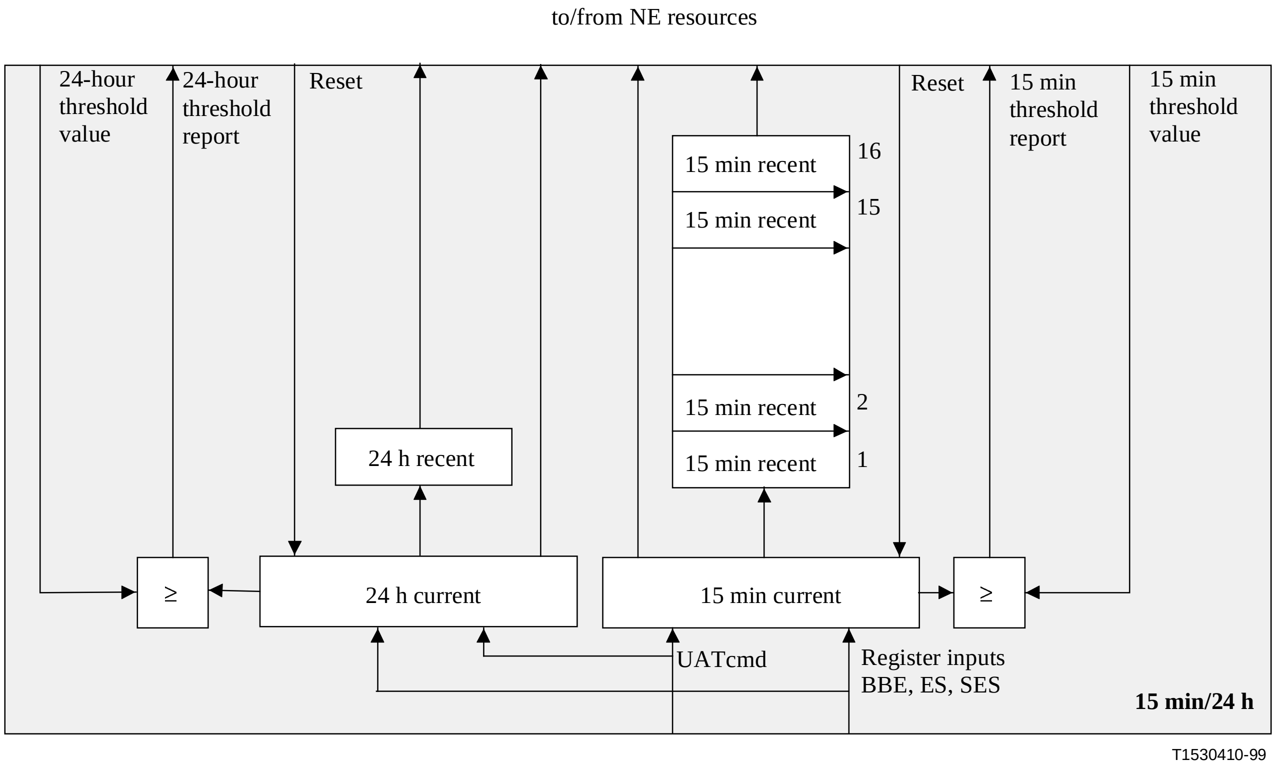
[3] A capability should be provided to ensure that, in the absence of reports, the reporting process is functioning properly.



a) The 15-minutes and 24-hour registers are optional for the unavailable seconds (UAS).

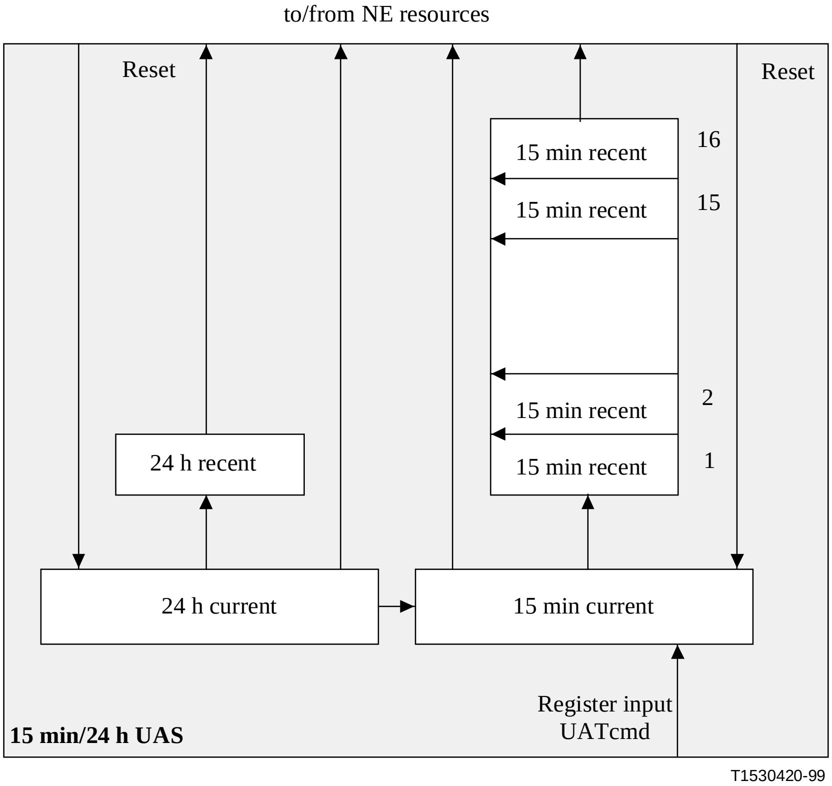
b) The determination of (un)available time introduces (functionally) a delay of 10 seconds. This delay should be considered when counting BBE, ES, SES.

Figure 7-5a/G.784 – Performance monitoring data collection and history for maintenance purposes



NOTE – The 15-minute and 24-hour current registers (15 min/24 h current) cumulate the content of the register with the register input value for seconds in available time. The register input value for seconds in unavailable time is ignored. UATcmd indicates (functionally) if a second is available or unavailable.

Figure 7-5b/G.784 – Registers process for maintenance based collection (ES, SES and BBE)



NOTE – The 15-minute current register (15 min current) cumulates the register with the register input value (UATcmd). UATcmd indicates if a second is unavailable.

Figure 7-5c/G.784 – Registers process for UAS (optional)

7.3.2.2 Performance data collection for error performance assessment purposes

This type of collection counts the events over fixed time periods of 24 hours only (Figure 7-6). Counting is stopped during unavailable time (see 7.3.3).

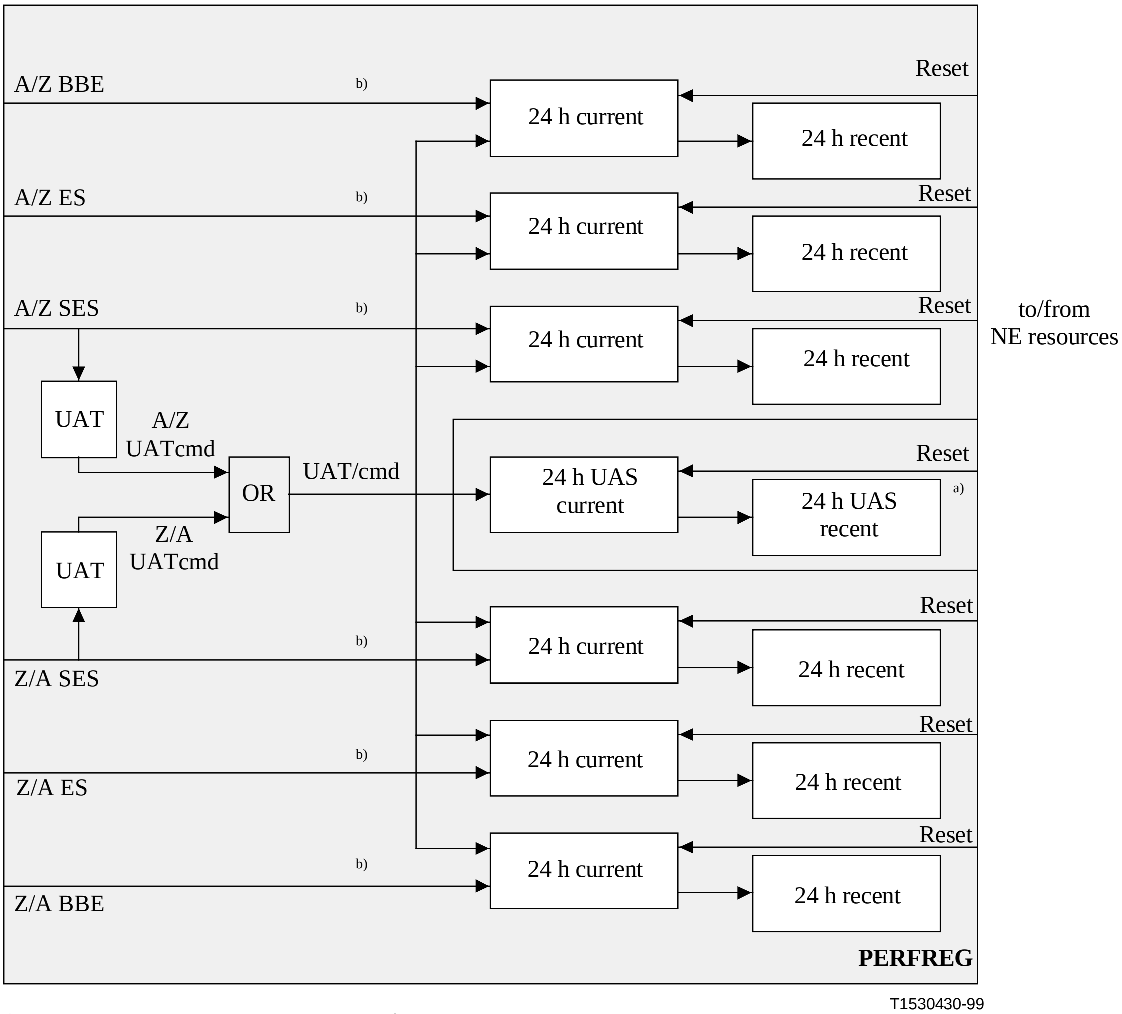
This counter operates as follows:

The performance events (e.g. SES) are counted in a counter per event type. These counters are called the current registers.

At the end of the 24-hour period the contents of the current registers are transferred to the recent registers (see 7.3.4), with a time-stamp to identify the 24-hour period, after which the current register shall be reset to zero.

It shall be possible to reset an individual current register to zero by means of an external command. The modularity of this command shall be as specified in Recommendation G.774.1.

Any register the content of which is suspect shall be flagged, using the "suspect interval flag" provided in Recommendation Q.822. This flag shall be raised independently for far-end and near-end counts. Examples of conditions to raise this flag are provided in Recommendation Q.822.



a) The 24-hour registers are optinional for the unavailable seconds (UAS).

b) The determination of unavailable time introduces (functionally) a delay of 10 seconds. This delay should be considered when counting BBE, ES, SES.

Figure 7-6/G.784 – Performance monitoring data collection and history for error performance assessment purposes

7.3.3 Performance data collection during unavailable time

The onset and exit of unavailable time is defined in Annex A/G.826 and in Recommendation M.2120. A period of unavailable time begins at the onset of ten consecutive SESs. These ten seconds are part of unavailable time.

A period of available time begins at the onset of ten consecutive non-SESs. These ten seconds are part of available time.

Performance monitoring event counting for ES, SES, and BBE shall be inhibited during unavailable time.

– In the performance data collection process for maintenance purposes, the unavailability of a single direction (see A.1/G.826) shall inhibit the counting for that direction only.

– In the performance data collection process for error performance assessment purposes, the unavailability of the bidirectional path (see A.2/G.826) shall inhibit the counting for both directions simultaneously.

7.3.4 Availability data collection

When a period of unavailability occurs, the beginning and ending of this period should be stored in a log in the NE, and as a consequence time-stamped. The time-stamp shall contain Day, Month, Year, Hour, Minute, Second information (refer to 2.3.7.2/M.2120).

The NE should be able to store these data in a log (see Recommendation G.774.1).

NOTE – The information in a log is not restricted to a single 24-hour period. For example, a log may contain periods of unavailability which are on the same day or on different days.

As an option, an additional unavailable second count (UAS) may be provided. Each second in unavailable time is defined to be an unavailable second. UASs are counted in 15-minute and in 24-hour counters.

In the performance data collection process for maintenance purposes, UAS counters exist per direction.

In the performance data collection process for error performance assessment purposes, only one UAS counter for both directions exists.

If a ten-second qualifying period preceeding the entry/exit of unavailability spans a register boundary, unavailability shall be entered/exited independently of the register boundary. This shall result in the entry/exit of unavailability, and associated inhibiting, at the beginning of the ten-second qualifying period.

The entry case is illustrated by:

period A	period B
- - - x_1 x_2 x_3 x_4	x_5 x_6 x_7 x_8 x_9 x_{10} x_{11} x_{12}

register boundary

"x" = SES, "-" = non-SES, x_1 to x_4 are in UAS register for period A, x_5 to x_{12} are in UAS register for period B.

7.3.5 Performance monitoring history

Performance history data are necessary to assess the recent performance of transmission systems. Such information can be used to sectionalise faults and to locate the source of intermittent errors.

Historical data, in the form of performance monitoring event counts, may be stored in registers in the NE or in mediation devices associated with the NE. For specific applications, for example when only Quality of Service alarms are used, historical data may not be stored.

All the history registers shall be time stamped.

The history registers operate as follows:

15-minute registers

The history of the 15-minute monitoring is contained in a stack of 16 registers per monitored event. These registers are called the recent registers.

Every 15 minutes the contents of the current registers are moved to the first of the recent registers. When all 15-minute registers are used, the oldest information will be discarded.

24-hour registers

The history of the 24-hour monitoring is contained in a single register per monitored event. This register is called the recent register.

Every 24 hours the contents of the current registers are moved to the recent register[4].

7.3.6 Use of thresholds

A thresholding mechanism can be used to generate an autonomous event report when the performance of a transport entity falls below a predetermined level. The general strategy for the use of thresholds is described in Recommendation M.20. Specific information is contained in Recommendations M.2101.1 and M.2120. The thresholding mechanism is applicable only for the maintenance based collection.

7.3.6.1 Threshold setting

The thresholds may be set in the NE, via the OS. The OS shall be able to retrieve and change the settings of the 15-minute and 24-hour thresholds.

The threshold values for events evaluated over the 15-minute period should be programmable with a range between 0 and a maximum value specified hereafter:

The maximum values for the number of events are[5]:

– 900 for the ES and SES events;

– $2^{16} - 1$ for the BBE event in the case of VC-11 up to VC-4 paths;

– $2^{24} - 1$ for the BBE event in the case of contiguous concatenated VC-4-Xc and STM-N ($X \leq 16$ and $N \leq 16$);

– $2^{16} - 1$ for each positive and negative counts of AU PJE.

The maximum values for the number of events evaluated over the 24-hour period shall be $2^{16} - 1$. The threshold value should be programmable between 0 and $2^{16} - 1$.

The value for STM-64 is for further study. The definition of a STM-64 multiplex section block is for under study in Study Group (SG) 13.

7.3.6.2 Threshold report

As soon as a threshold is reached or crossed in a 15-minute/24-hour period for a given performance event, a threshold report (TR) is generated.

As an option for 15-minute periods, an alternative method of threshold reporting can be used. When for the first time a threshold is reached or crossed for a given performance event, a threshold report is generated. No threshold reports will be generated in subsequent 15-minute periods until a clear threshold is undercrossed for the performance event. Then, a reset threshold report (RTR) is generated.

The detailed functioning of the threshold mechanisms is explained in 2.3/M.2120.

Performance data shall be reportable across the NE/OS interface automatically upon reaching or crossing a performance monitoring threshold.

---

[4] This implies that all 24-hour data is discarded after 24 hours.

[5] The maximum values for BBE events for VCs and STM-Ns is smaller than the maximum number of BBEs that could theoretically be detected in a 15-minute period.

7.3.7 Performance data reporting

Performance data stored in the NE may be collected by the OS for analysis without affecting the content of the register.

7.3.7.1 Access by the OS to the performance data

Performance data shall be reportable across the OS/NE interface on demand when requested by the OS.

7.3.7.2 Periodical report of performance data

Data collection may be performed periodically to support trend analysis to predict future failure or degraded conditions. On request of the OS, performance data of specific ports shall be reportable periodically.

7.3.8 Additional monitored events

Additional counts such as OFS, AU PJE, CSES, ESA, ESB and FC may be useful. Their implementation is optional (see Table 7-2). The OFS, AU PJE, ESA, ESB, and FC event counts may be stored in 15-minute and 24-hour registers, as detailed in 7.3.2.1 and 7.3.5.

The Out-of-Frame Second (OFS) is declared when the STM-N frame alignment process is in the OOF state at least once in the second. Refer to Recommendation G.783. The AF communicates this via the MI_pOFS signal to the EMF.

If AU PJE counters are provided, then positive and negative PJEs shall be counted separately on one selectable AU within an STM-N signal, after the AU has been resynchronized to the local clock. Refer to Recommendation G.783. The number of positive and negative outgoing PJEs per second is communicated from the AF to the EMF via the MI_pPJE+ and MI_pPJE – signals.

The CSES event occurs when a sequence that contains X or more consecutive SES is detected. The sequence is terminated by an unavailable period or when a second that is not a SES is encountered. The NE should be able to store these time-stamped CSES data in a log (see Recommendation G.774.1); the time-stamp shall indicate the time of the first SES in the sequence. The value of X may be configured by an OS in the range of 2 to 9. When a sequence of consecutive SESs is terminated by the entry into an unavailable period, the CSES event is not recorded.

The following PM parameters may also be provided: Errored Seconds – Type A (ESA), Errored Seconds – Type B (ESB), and Failure Counts (FC). These parameters are defined in Annex A, and their implementation is optional per country.

ESA and ESB can be used in addition to Errored Seconds (ES) to delineate dribbling error patterns from short burst error patterns. At international boundaries, they are only used if there is mutual agreement among the network operators involved to provide these parameters, and if the participating countries also support them.

Failure Counts can be used to determine whether a UAS or SES count is the result of a single failure or multiple failures. At international boundaries, it is only used if there is mutual agreement among the network operators involved to provide this parameter, and if the participating countries also support it.

Table 7-2/G.784 – SDH additional monitored events

Monitored events	RS	MS	Path HOVC	Path LOVC
OFS	O			
CSES	O	O	O	O
AU PJE			O	
ESA		OC	OC	OC
ESB		OC	OC	OC
FC		OC	OC	OC

O	Optional
OC	Optional per Country and per Carrier
AU PJE	Administrative Unit Pointer Justification Event
OFS	Out-of-Frame Second
CSES	Consecutive SES counts configurable in the range of 2 to 9 SES
ESA	Errored Seconds Type A
ESB	Errored Seconds Type B
FC	Failure Counts

7.3.9 Performance monitoring resource assignment

Performance monitoring within a network element is a set of processes that can be completely absent, 100% present, or available for a limited percentage. Figure 7-7 illustrates this:

– there is the set of trail termination sink functions within the network element (shown at the left side of the figure);

– a (sub)set of the termination sink functions is connected with the performance monitoring resource assignment function (a kind of "connection" function);

– there is a set of performance monitoring processes[6] (right side of the figure) within the network element;

– within the limitations of this network element, connections can be made and removed between termination sink functions and performance monitoring processes.

[6] These performance monitoring processes might be of different types. Refer to Appendix I.

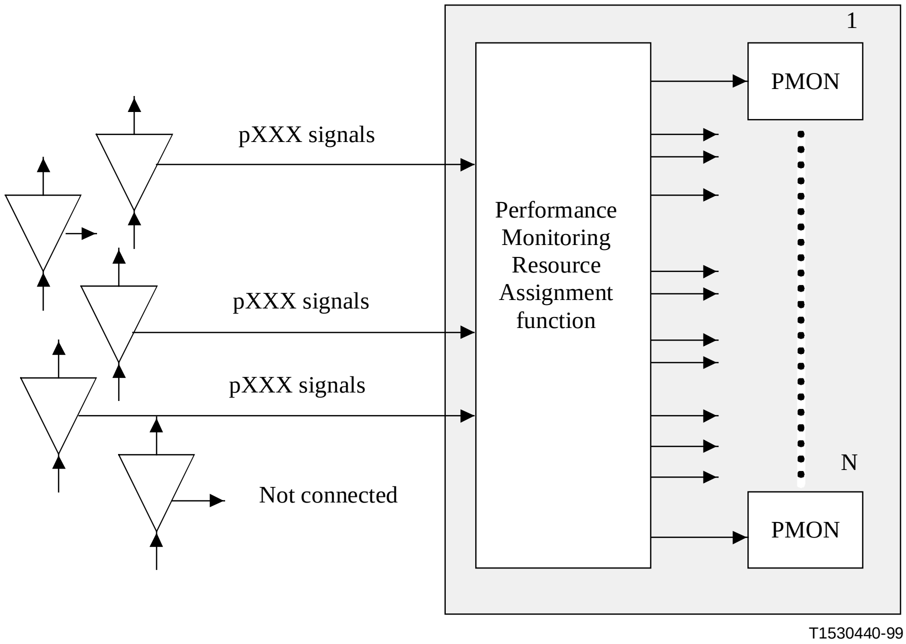


Figure 7-7/G.784 – Performance monitoring resource assignment

Several types of performance monitoring processing are specified (see Appendix I) differing in characteristics like: unidirectional or bidirectional, near-end or far-end, terminating node or intermediate node. The SEMF may support one or more of these types.

7.4 Configuration management

7.4.1 Provisioning (protection switching)

Network elements may support one or more types or protection (linear MSP, MS SPring, SNCP, VC trail protection), each of which can be characterized by the set (or a subset) of the following parameters:

– protection architecture (1+1, 1:n, m:n);

– switching type (unidirectional, bidirectional);

– operation type (non-revertive, revertive);

– Automatic Protection Switch (APS) channel (provisioning, usage, coding);

– protection switch requests;

– protection switch performance;

– protection switch state machine.

The protection switching scheme of an SDH network element can be set up autonomously by the network element, according to its make-up and mode of operation, or it may be done by means of external provisioning.

7.4.1.1 Linear STM-N MS protection

The functions which allow the user to provision the configuration of the protection scheme are:

– establishment of protection, indicating the protection switching mode (uni/bidirectional) operation mode (revertive/non-revertive), extra traffic (supported, not supported), the entities participating in the protection, their role (working/protection), and possibly their priority;

– modification of protection, adding or removing entities and/or modifying their protection characteristics;
– suppression of protection;
– wait-to-restore time;
– SF and SD priority;

This information is conveyed between the EMF and an AF via the MI_SWtype, MI_OPERtype, MI_EXTRAtraffic, MI_WTRtime, MI_SFpriority, MI_SDpriority (see Table 7-3).

Table 7-3/G.784 – Linear MSP related provisioning

MI signal	Value range	Default value
switching type (MI_SWtype)	unidirectional, bidirectional	No default defined
operation type (MI_OPERtype)	revertive, non-revertive	No default defined
extra traffic (MI_EXTRAtraffic)	true, false	No default defined
wait-to-restore time (MI_WTRtime)	0,1,..,12 minutes	5 minutes
priority of SF and SD conditions in 1:n MSP (MI_SFpriority, MI_SDpriority)	high, low	high

7.4.1.2 STM-N MS SPring protection

For further study.

7.4.1.3 Linear 1+1 SNC protection

The functions which allow the user to provision the configuration of the protection scheme are:

– establishment of protection, indicating the operation mode (revertive/non-revertive), SNC protection type (SNC/I, SNC/N), the entities participating in the protection, their role (working/protection);
– modification of protection, adding or removing entities and/or modifying their protection characteristics;
– suppression of protection;
– wait-to-restore time, hold off time.

This information is conveyed between the EMF and an AF via the MI_OPERtype, MI_WTRtime, MI_HOtime, MI_PROTtype (see Table 7-4).

Table 7-4/G.784 – Linear SNCP related provisioning

MI signal	Value range	Default value
operation type (MI_OPERtype)	revertive, non-revertive	non-revertive
protection type (MI_PROTtype)	SNC/I, SNC/N	No default defined
wait-to-restore time (MI_WTRtime)	0,1,..,12 minutes	5 minutes
hold off time (MI_HOtime)	0, 100 ms, 200 ms,..,10 s	0

7.4.1.4 Linear 1+1 VC Trail protection

The functions which allow the user to provision the configuration of the protection scheme are:

– establishment of protection, indicating the protection operation mode (revertive/non-revertive), the entities participating in the protection, their role (working/protection);

– modification of protection, adding or removing entities and/or modifying their protection characteristics;

– suppression of protection;

– wait-to-restore time, hold off time.

This information is conveyed between the EMF and an AF via the MI_OPERtype, MI_WTRtime, MI_HOtime (see Table 7-5).

Table 7-5/G.784 – Protection related provisioning

MI signal	Value range	Default value
operation type (MI_OPERtype)	revertive, non-revertive	non-revertive
wait-to-restore time (MI_WTRtime)	0,1,..,12 minutes	5 minutes
hold off time (MI_HOtime)	0, 100 ms, 200 ms,..,10 s	0

7.4.2 Status and control (protection switching)

The general facility of protection switching is defined as the substitution of a standby or backup facility for a designated facility. The functions which allow the user to control the traffic on the protection line are:

– operate/release manual protection switching;

– operate/release force protection switching;

– operate/release lockout;

– request/set automatic protection switching (APS) parameters.

This information is conveyed between the EMF and an AF via the MI_EXTCMD signal (see Table 7-6).

Table 7-6/G.784 – Protection related control provisioning

MI signal	Value range	Default value
external command (MI_EXTCMD)	CLR, LO, FSw, MSw, EXER	None

7.4.3 Installation functions

For further study.

7.4.4 Provisioning and reporting (trace identifier processes)

The functions which allow the user to provision the operation of a trace identifier process are:

– provisioning of source API;

– provisioning of the expected API;

– enable/disable detection of dTIM.

The source and expected APIs are communicated from the EMF to an AF via the MI_TxTI and the MI_ExTI signals. The detection mode for dTIM is communicated from the EMF to an AF via the MI_TIMdis signal (see Table 7-7).

An AF will report on request of the EMF the value of the received and accepted TTI via the MI_AcTI signal.

The interface between the EMF and the MCF (and element management system) is for further study.

Table 7-7/G.784 – Trace Identifier related provisioning and reporting

MI signal	Value range	Default value
MI_TxTI	According to Rec. G.707	N/A
MI_ExTI	According to Rec. G.707 (Note 1)	N/A
MI_TIMdis	False, true	(Note 2)
MI_AcTI	According to Rec.G.707 (Note 1)	N/A
NOTE 1 – The interworking with equipment not supporting trace identifier insertion is for further study. NOTE 2 – There are various network scenarios which require different default settings.		

7.4.5 Provisioning and reporting (payload structures)

Access Points which have multiple adaptation functions connected to it, allowing different client signals to be transported via the server signal, need a selection of the active client. This is controlled via the activation/deactivation of adaptation functions via the MI_Active signals (see Table 7-8).

NOTE – For cases where an access point has a single adaptation function connected and supports a single client signal only, the MI_Active signal is fixed active.

An AF will report on request of the EMF the value of the received and accepted payload type signal via the MI_AcSL signal.

Table 7-8/G.784 – Payload type related provisioning and reporting

MI signal	Value range	Default value
MI_Active	true, false	false
MI_AcSL	application dependent	N/A

7.4.6 Provisioning (matrix connections)

A connection function is surrounded by Connection Points (CP) and Termination Connection Points (TCP). Each TCP is identified via the API associated with its Trail Termination function, and each CP is identified via the API associated with its Adaptation function, extended with a (if applicable) tributary signal number (Figures 7-8a, 7-8b and 7-8c).

For the case of a trail protection, the Access Points (AP) are named as follows: AP of working #i and AP of normal #i have the same AP Identifier, AP of protection has a separate AP identifier, AP of extra traffic has the same AP Identifier as the AP of protection. This maintains the CPId's when the interface changes from unprotected to protected and vice versa.

The relation with the information model naming scheme defined in Figures A.2/G.774 and A.3/G.774 is as follows:

- APId, TCPId are represented by the TTP.
- CPId is represented by the CTP.

A matrix connection is therefore characterized by its (T)CP Ids communicated between EMF and AF via the MI_ConnectionPortIds signal. The connection type is communicated via MI_ConnectionType and directionality via MI_Directionality signals (see Table 7-9).

Table 7-9/G.784 – Matrix connection related provisioning

MI signal	Value range	Default value
MI_ConnectionPortIds	Set of (T)CP Ids	No default defined
MI_ConnectionType	unprotected, 1+1 protected, ...	No default defined
MI_Directionality	unidirectional, bidirectional	No default defined

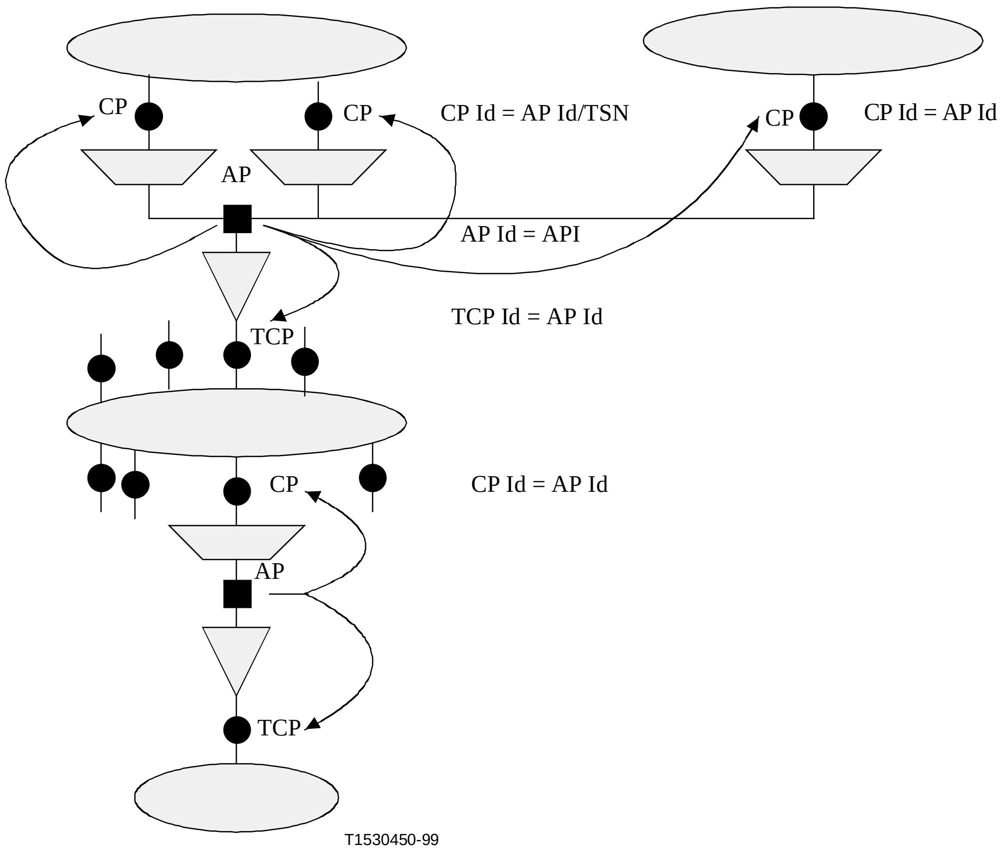


Figure 7-8a/G.784 – CP and TCP Identification scheme

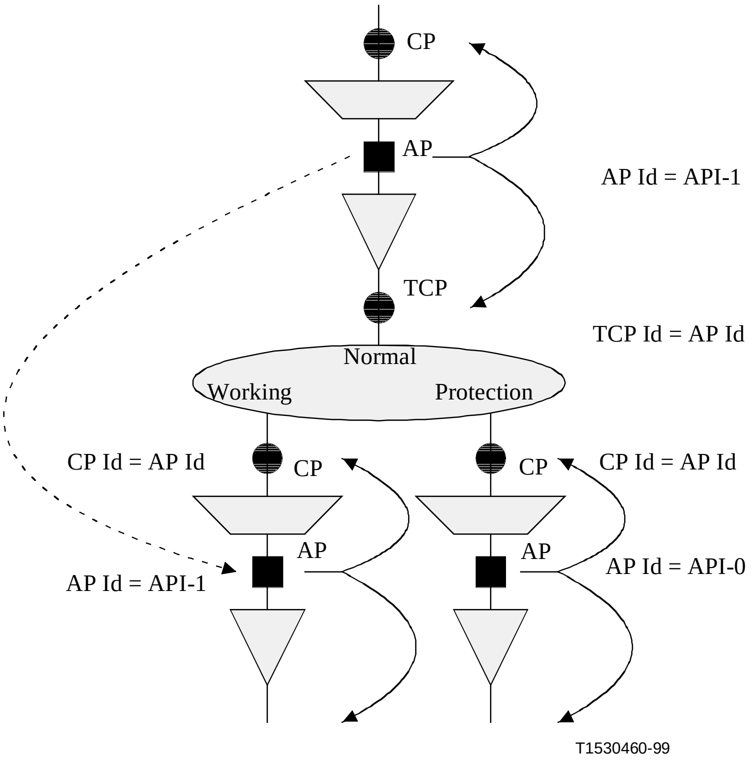


Figure 7-8b/G.784 – CP and TCP Identification scheme for case of 1+1 trail protection

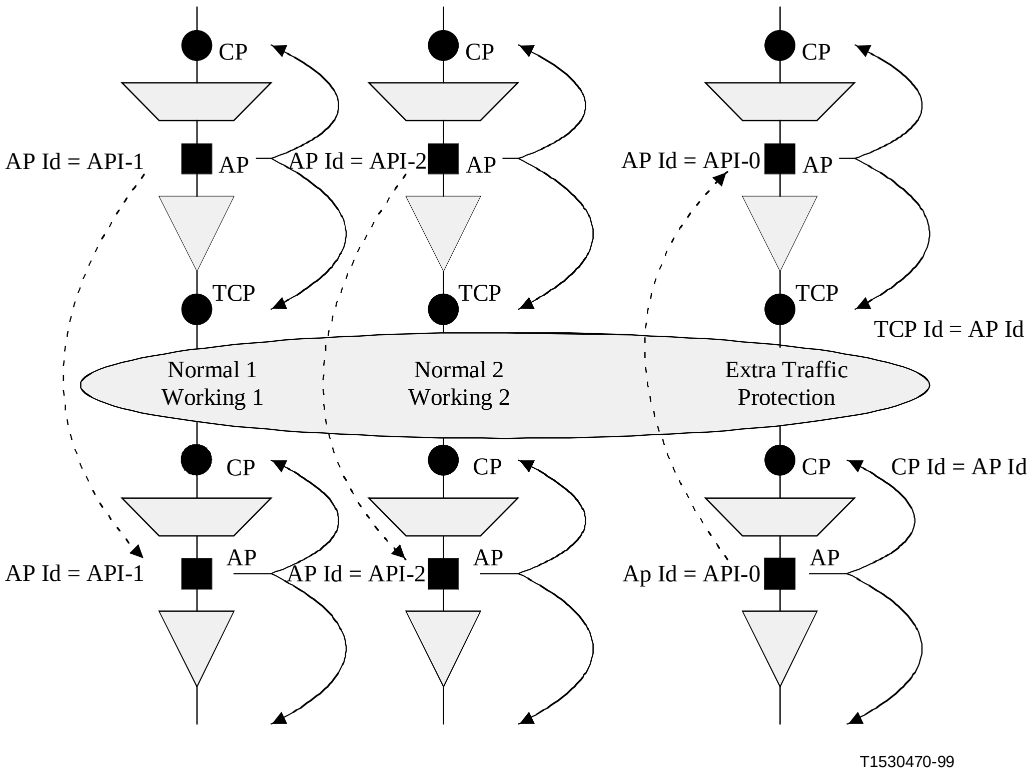


Figure 7-8c/G.784 – CP and TCP Identification scheme for case of 1:n trail protection

7.4.7 Provisioning (EXC/DEG thresholds)

The thresholds of Poisson based Excessive and Degraded defect detector processes, and the threshold and monitor period of the burst based Degraded defect process requires provisioning. This information is communicated between the EMF and an AF via the MI_EXC_X, MI_DEG_X (Poisson case) and MI_DEGTHR, MI_DEGM (burst case) signals (see Table 7-10).

Table 7-10/G.784 – Error defect detection related provisioning

MI signal	Value range	Default value
Poisson based excessive defect threshold selection (MI_EXC_X)	10^{-3},10^{-4}, 10^{-5}	10^{-3}
Poisson based degraded defect threshold selection (MI_DEG_X)	10^{-5}, 10^{-6}, 10^{-7}, 10^{-8}, 10^{-9}	10^{-6}
Burst based degraded defect interval threshold selection (MI_DEGTHR)	0..100% or 0..N EBs (Note)	SES threshold
Burst based degraded defect monitor period selection (MI_DEGM)	2..10	7
NOTE – The granularity for the degraded defect threshold selection is for further study. See 2.2.2.5.2/G.783.		

The granularity of these signals is outside the scope of this Recommendation. Examples are:

– global per network element;

– global per network layer in the network element;

– global per server/aggregate signal in the network element;

– individual per trail/signal in the network element.

The two extremes are "provisioning per individual signal" and "provisioning per network element". The first example offers full flexibility with relative high complexity in equipment and in management. The second example offers low complexity in equipment and in management with very limited flexibility.

An equipment will support one or more of these options, depending on the intended application of the equipment in the network.

7.4.8 Provisioning and reporting (Portmode, TPmode)

The TPmodes and Portmodes (see 2.2.1/G.783) of trail termination sink functions (i.e. the end-to-end path termination, non-intrusive monitor, supervisory-unequiped termination, end-to-end tandem connection termination, and tandem connection non-intrusive monitor) require provisioning. This information is communicated between the EMF and an AF via the MI_Portmode and/or MI_TPmode signals (see Table 7-11).

When supported, the Portmode may change automatically from AUTO state to MON state on clearing of the port's LOS defect.

Table 7-11/G.784 – Port and Termination Point mode related provisioning

MI signal	Value range	Default value
Port mode control (MI_Portmode)	MON, (AUTO), NMON	AUTO (if supported) otherwise NMON
Termination Point mode control (MI_TPmode)	MON, NMON	NMON

7.4.9 Provisioning (XXX_Reported)

The reporting of the following defects is an option: AIS, RDI, ODI. These defects are "secondary defects" in that they are the result of a consequent action on a "primary defect" in another network element. This is controlled by means of the parameters MI_AIS_Reported, MI_RDI_Reported, and MI_ODI_Reported (see Table 7-12).

Table 7-12/G.784 – Consequential defect/failure related provisioning

MI signal	Value range	Default value
MI_AIS_Reported	true, false	false
MI_RDI_Reported	true, false	false
MI_ODI_Reported	true, false	false

The granularity of these signals is outside the scope of this Recommendation. Examples are:

– global per network element;

– global per network layer in the network element;

– global per server/aggregate signal in the network element;

– individual per trail/signal in the network element.

The two extremes are "provisioning per individual signal" and "provisioning per network element". The first example offers full flexibility with relative high complexity in equipment and in management. The second example offers low complexity in equipment and in management with very limited flexibility.

An equipment will support one or more of these options, depending on the intended application of the equipment in the network.

7.4.10 Provisioning and reporting (Synchronization)

NOTE – Enhancement of G.783 synchronization specifications is under study. These specifications will be replaced by Recommendation G.781. The next revision of synchronization provisioning and reporting within Recommendation G.784 will be based on Recommendation G.781.

The functions which allow the user to provision the operation of the synchronization process are:

– provisioning for selector A of a fall-back order. This fall-back order is a list of a set of T1 synchronization signals in a priority order for generation of external synchronization signal T4;

– provisioning for selector C of a fall-back order. This fall-back order is a list of (a set of) T1, T2 or T3 synchronization signals in a priority order for generation of internal synchronization signal T0 by the SETG;

– selection of either T0 or output of selector A for generation of external synchronization signal T4;

– activation/deactivation of T4 squelching;

– selection of SETG when SETG is replicated.

The synchronization function reports to the EMF (see Table 7-13):

– which synchronization signal is selected by selector A;

– which synchronization signal is selected by selector B;

– which synchronization signal is selected by selector C;

– the status of the synchronization signal inputs (T1, T2, T3);

– the status of the SETG (i.e. freerunning, holdover or locked mode);

– the selected SETG when SETG is replicated.

Table 7-13/G.784 – Synchronization related provisioning and reporting

MI signal	Value range	Default value
MI_FallBackOrderA (selector A)	Set of sync sources Id in priority order	No default value
MI_FallBackOrderB (selector B)	Set of sync sources Id in priority order	No default value
MI_SelectT4 (selector C)	Set of sync sources Id	No default value
MI_SquelchT4 (selector C)	on, off	off
MI_SelectSETG (if SETG replicated)	SETG#1, SETG#2	SETG#1
MI_SelectedInput (for selectors A, B & C)	Set of sync sources Id	N/A
MI_InputStatus	normal, failed (LOS, AIS)	N/A
MI_SETGSelected (if SETG replicated)	SETG#1, SETG#2	N/A
MI_SETGStatus	freerunning, holdover, locked	N/A

7.5 Security management

For further study.

8 Protocol stack

8.1 Description

The protocol stack specified in this clause has been selected to satisfy requirements for the transfer of operations, administration, maintenance and provisioning (OAM&P) messages across the SDH data communications channels (DCC). It is in accordance with the current object oriented approach to the management of open systems.

8.1.1 ECC protocol stack description

The protocols for each layer, as outlined in the following subclauses, are to be used for management communications over the SDH ECC. The specifications of these protocols are given in 8.2.

8.1.1.1 Physical layer (layer 1)

The SDH data communications channel (DCC) constitutes the physical layer.

8.1.1.2 Data link layer (layer 2)

The data link protocol, LAPD (see Recommendation Q.921 [6]) provides point-to-point connections between nodes of the underlying transmission network.

8.1.1.3 Network layer (layer 3)

The network protocol ISO 8473 [1] provides a datagram service suitable for the higher speed, high quality underlying network. Convergence protocols have been defined in ISO 8473 [1] for the operation of ISO 8473 [1] over both connection-oriented and connectionless data link subnetworks.

8.1.1.4 Transport layer (layer 4)

The transport protocol ensures the accurate end-to-end delivery of information across the network. The protocol creates a transport connection from the underlying connectionless network service (see ISO/IEC 8073/Add.2 [3]) over both connection-oriented and connectionless data link subnetworks.

8.1.1.5 Session layer (layer 5)

The session protocol ensures that the communications systems are synchronized with respect to the dialogue underway between them and manages, on behalf of the presentation and application layers, the transport connections requires.

8.1.1.6 Presentation layer (layer 6)

The presentation layer and the ASN.1 basic encoding rules act to ensure that application layer information can be understood by both the communicating systems, the context of the information being transferred and the syntax of the encoding of information.

8.1.1.7 Application layer (layer 7)

The following options of the application layer shall be utilized:

i) *CMISE*

The common management information service element (CMISE) of the ISO common management information protocol (CMIP) ISO/IEC 9596 [4] provides services for the manipulation of management information across the ECC.

ii) *ROSE*

The remote operations service element (ROSE) permits one system to invoke an operation on another system and to be informed of the results of that operation.

iii) *ACSE*

The association control service element (ACSE) provides services to initiate and terminate a connection (association), between two applications.

8.2 Protocol specifications

This subclause specifies protocols for the SDH ECC. Where possible, the protocols are specified by reference to Q.811 [7] or Q.812 [8], the lower and upper layer profiles for the Q3 interface. Layer 1, layer 2 and additional parameters for layer 3 are specified here. All other specifications refer to Q.811 [7] or Q.812 [8].

Protocol options, features, parameter values, etc., in addition to those specified in this Recommendation may be included in a conforming system provided they are not explicitly excluded by this Recommendation and they do not prevent interoperability with conforming systems that do not provide them.

A control network topology is outlined in 5.2.2.

8.2.1 Physical layer protocol specification

The regenerator section DCC shall operate as a single 192 kbit/s message channel using the section overhead bytes D1 to D3. The multiplex section DCC shall operate as a single 576 kbit/s message channel using the section overhead bytes D4 to D12.

8.2.2 Data link layer protocol specification

The data link layer shall provide point-to-point transfer, over the SDH DCC, of Network Service Data Units through a single or multiple[7] logical channel between each pair of adjacent network nodes.

The data link layer shall operate under the rules and procedures specified in Recommendation Q.921 [6] for the Unacknowledged information transfer service specified in 8.2.2.1, and for Acknowledged information transfer service specified in 8.2.2.2. Both services (UITS and AITS) shall be supported. AITS shall be the default mode of operation.

A mapping between the connection-mode Data Link service primitives defined in ISO/IEC 8886 [9] (Recommendation X.212 [9]) and Recommendations Q.920 [5] and Q.921 [6] primitives is defined in Table 8-1.

8.2.2.1 Unacknowledged information transfer service

UITS shall follow the rules and procedures specified in Recommendation Q.921 [6]. For the UITS, the subnetwork dependent convergence function provides a direct mapping onto the data link layer as specified in 8.4.4.1/ISO 8473/Add.3 [2]. For this application, mandatory and optional service and protocol parameters shall have the values specified in Table 8-2.

8.2.2.2 Acknowledged information transfer services (AITS)

AITS shall follow the rules and procedures specified in Recommendation Q.921 [6]. For AITS, the subnetwork dependent convergence function provides a mapping onto the data link layer as specified in 8.4.4.2/ISO 8473/Add.3 [2]. For this application, mandatory and optional service and protocol parameters shall have the values specified in Table 8-3. In addition, the requirements specified in c) to f) of Table 8-2 shall also be followed. The default values defined in Table 8-3 may not be suitable for high delay (satellite) applications.

Table 8-1/G.784 – Mapping of Data Link service and Q.920 [5] primitives

Data Link Service Primitive	Q.920 Primitive
DL-CONNECT request DL-CONNECT indication DL-CONNECT response DL-CONNECT confirm	DL-ESTABLISH request DL-ESTABLISH indication (Notes 1 and 2) DL-ESTABLISH confirm
DL-DATA request DL-DATA indication	DL-DATA request DL-DATA indication
DL-DISCONNECT request DL-DISCONNECT indication (Note 3)	DL-RELEASE request DL-RELEASE indication DL-RELEASE confirm
NOTE 1 – This primitive indicates that the data link connection is open. NOTE 2 – Recommendation Q.921 will ignore this response. NOTE 3 – Network layer will ignore this confirmation.	

[7] The use of multiple logical channels is recommended for circuits with a high propagation delay.

Table 8-2/G.784 – UITS specification

a)	The unnumbered information (UI) frames shall be used for data transfer as specified in Recommendation Q.921 [6].
b)	As specified in Recommendation Q.921 [6], UI frames shall always be commands. The assignment of user-side/network-side roles (and hence the C/R bit value) shall be made prior to initialization.
c)	Access point identifier (SAPI) Value: 62[a)]
d)	Terminal end-point identifier (TEI) Value: 0 (Note)
e)	Frame size shall be capable of supporting an Information Field of 512 octets as specified in 8.4.2/ISO 8473 [1].
f)	Management procedure, as specified in Recommendation Q.921 [6], shall not be supported.
g)	Poll/Final Bit shall always be set to 0, as specified in Recommendation Q.921 [6].

[a)] The need for additional SAPIs is for further study, e.g. to support SDH DCC.

NOTE – Recommendations Q.921 [6] and Q.922 [10] specify that implementations must route on the two-octet address field. Currently two applications use SAPI = 62, SDH ECC (TEI = 0) and frame relay maintenance (TEI = 127).

Table 8-3/G.784 – AITS specifications

a)	Assignment of user-side/network-side roles, and hence the C/R bit value, shall be made prior to initialization.
b)	The default value for (k): 7 (127 for satellite applications) (Note 1)
c)	The default value for T200: 1 second
d)	The default value for T203: 10 s (Note 2)
e)	The default value for N200: 3
f)	Data link monitor functions as specified in Recommendation Q.921 [6] are optional.
g)	Negotiation as described in Appendix IV/Q.921 [6] may be used to select alternative parameter values.

NOTE 1 – For satellite parameters, the above default are application-specific and may be modified e.g. using the XID frames. Note also that for satellite use the maximum TPDU should be 1024 bytes for DCC_R and 4096 bytes for DCC_M.

NOTE 2 – This parameter is used with the optional procedures listed as item f).

8.2.3 Network layer protocol specification

The network layer protocol shall be ISO 8473 [1] as specified in 5.3.3/Q.811 [7]. In addition, the Quality of service maintenance function shall be used for the selection of AITS or UITS service at layer 2. The QoS parameter shall be used as specified in 6.16/, 7.5.6/ and 7.5.6.3/ISO 8473 [1]. The coding of the QoS parameter for the selection of UITS/AITS is shown below:

1) The absence of a QoS parameter shall select AITS in the data link.
2) In the QoS parameter, bits 7 and 8 set to 1 (globally unique QoS) and bit 1 set to 1 shall select AITS.
3) In the QoS parameter, bits 7 and 8 set to 1 (globally unique QoS) and bit 1 set to 0 shall select UITS.
4) The use of QoS parameter bits 2, 3, 4, 5 and 6 are not the subject of, or specified in, this Recommendation.

The criteria for selecting AITS or UITS is the network provider's responsibility.

8.2.4 Transport layer protocol specification

The required transport layer protocol shall be class 4 operation as specified in 3.2/Q.812 [8].

8.2.5 Session layer

The session layer shall be as specified in 3.3/Q.812 [8].

8.2.6 Presentation layer

The presentation layer shall be as specified in 3.4/Q.812 [8].

8.2.7 Application layer

The application layer shall be as specified in 3.5/Q.812 [8]. Support of the file transfer, access and management (FTAM) protocol is not required.

9 ECC interworking

9.1 Introduction

Within the TMN architecture (see Recommendation M.3000), the SMS is a type of local communications network (LCN). Communications between an SMS and OS will take place (optionally) over one or more intervening wide-area data communications networks (DCN) and LCNs. Therefore, interworking is necessary between the SMS and either a DCN or another LCN. Interworking may also be necessary between a DCN and an LCN. This clause will only specify the interworking between a SMS and DCN.

The regenerator section and multiplex section DCCs will use the seven layer, OSI protocol stack specified in clause 8 and includes the connectionless-mode network protocol (CLNP) that is specified in ISO 8473 [1]. For the purpose of this Recommendation, the communications on the DCN between the OS and entry point(s) to the SMS will use an OSI protocol stack that includes the X.25 connection-mode network protocol (CONP) specified in ISO/IEC 8208 with ISO IP (ISO 8473 [1]) as an option in the OS.

The OSI architecture describes the view that interworking between subnetworks, such as the SMS and DCN, should take place within the network layer, with the transport and higher layers operating strictly on a peer-to-peer basis between end systems (SNE and OS). ISO 7498 specifies that the network layer will provide the transparent data transfer between transport-entities, i.e. end systems, that is independent of the characteristics, other than quality of service, of different subnetworks. This is identified as the routing and relaying function in the network layer. ISO 8648 specifies the OSI principles of interworking within sublayers of the network layer.

9.2 Interworking between the SMS and DCN

Interworking between the SMS's CLNP and the DCN's CONP OSI protocol stacks shall be required. Interworking, at the lower layers, between the SMS's and the DCN's OSI protocol stacks shall be based upon ISO TR 10172. The ISO interworking TR defines an interworking functional unit (IFU) that will perform relaying and/or conversion of PDUs between networks.

9.3 Network layer relay overview

The IFU, operating in the NLR mode, would function as a regular intermediate system and is the only OSI compliant method of interworking between end systems with different OSI network protocols. As specified in ISO 7498 and ISO 8648, interworking is a network layer function. ISO 8473 [1] specifies the CLNP and describes an SNDCF that specifies the rules for operating the CLNP over an X.25 packet switched network (PSN).

The NLR could provide interworking between the SMN and the DCN if both the SMN and DCN operated the ISO 8473 [1] CLNP and utilized TP class 4 (TP4) connections. The top-level SMS SNE – DCN OS network service would then be connectionless, with the X.25 PSN providing an underlying CONP from the IFU to the OS via the DCN. The IFU would examine the destination address of network PDUs (NPDU) received from the SMN and then transfer those CLNP NPDUs (from the SMS) to an appropriate X.25 switched virtual circuit (SVC) on the DCN.

10 Operations interfaces

10.1 Q-interface

For interconnection with the TMN, the SMS will communicate through a Q-interface having a protocol suite, B1, B2 or B3 as defined in Recommendation G.773. The selection of which of the three protocol suites to adopt is a network provider's decision.

10.2 F-interface

For further study.

ANNEX A

Definitions of Errored Seconds Types A and B and Failure

A.1 Introduction

This annex provides definitions of the following optional performance management parameters: Errored Seconds – Type A (ESA), Errored Seconds – Type B (ESB) and Failure Counts (FC).

A.2 Errored Seconds – Type A and B

The optional ESA and ESB parameters can be used in addition to Errored Seconds (ES) and Severely Errored Seconds (SES) to help maintain quality service by delineating dribbling error patterns from short burst error patterns. ESA and ESB separate errored seconds that have one error from those that have more than one error (but not enough errors to become a SES). Two applications of ESA and ESB are provided below.

Example 1: Proactive Maintenance

To provide high quality service to customers, extra maintenance measures need to be employed. Waiting until a facility fails outright does not satisfy customers in general. Different types of facilities have distinct failure and error patterns, and in many cases the failure occurs only after a protracted period of errored seconds. By monitoring these ESA and ESB, and SES occurrences, and knowing the failure signature of a given facility, maintenance of the system can be scheduled in a timely manner well in advance of a hard failure.

Example 2: Work Lists

There are often more facility problems that occur than the available maintenance technical force can handle. Thus a means is needed to determine which facility problems are worked first. The analysis of ESA, ESB and SES provides one of these means. For example, given two facilities with errors, one with Type A and the other with Type B, a technician would select the facility with Type B errors to repair first because it is causing a more degraded service to a customer than the system with Type A errored seconds.

Definitions

ESA and ESB for both multiplex section and VC path layers are defined below.

Errored Second A (ESA): This parameter is a count of the 1-second intervals containing a single errored block, and none of the specific defects listed below:

- OOF, LOS for regenerator sections.
- AIS for multiplex section near-end.
- RDI for multiplex section far-end.
- AIS, LOP for higher order and lower order virtual containers.
- RDI for higher order and lower order virtual containers.

Errored Second B (ESB): This parameter is a count of the 1-second intervals containing more than a single errored block, less than the number of errored blocks that is required to declare an SES, and none of the specific defects listed below:

- OOF, LOS for regenerator sections.
- AIS for multiplex section near-end.
- RDI for multiplex section far-end.
- AIS, LOP for higher order and lower order virtual containers.
- RDI for higher order and lower order virtual container.

These two parameters follow the same rules as ESs with regard to count increments during Unavailable Time.

A.3 Failure Counts

The optional Failure counts are used to determine whether a UAS or SES count is the result of a single failure or multiple failures. For example, during a 15-minute interval, 600 s of unavailable time are counted, and the failure count indicates 20 failures. In such a scenario, because the unavailable time is not due to a single failure, the maintenance craft considers the failure as more severe, and generally takes a more time consuming fault analysis approach.

Definitions

The failure counts and the corresponding failure events for both multiplex section and VC path layers are defined below.

Near-end Failure Count: This parameter is a count of the number of occurrences of near-end failure events, and is incremented by one each time a near-end failure event begins.

As an example, MS near-end failure events begin when an MS-AIS is declared, and path near-end failure events begin when a LOP or path-AIS is declared.

Far-end Failure Count: This parameter is a count of the number of occurrences of far-end failure events, and is incremented by one each time a RDI event begins.

Failure counts are incremented during unavailable time.

APPENDIX I

Performance monitoring applications

Multiple (different) applications of performance monitoring are defined in 5.3. Each application requires a different configuration of the performance monitor processes specified in 5.3. Several of these configurations are presented in Figure I.1.

Figure I.1 a) illustrates the performance monitoring process configuration at node Z (tail end) supporting a unidirectional (maintenance) application for the single direction (A-to-Z); it uses near-end performance monitoring primitives as input.

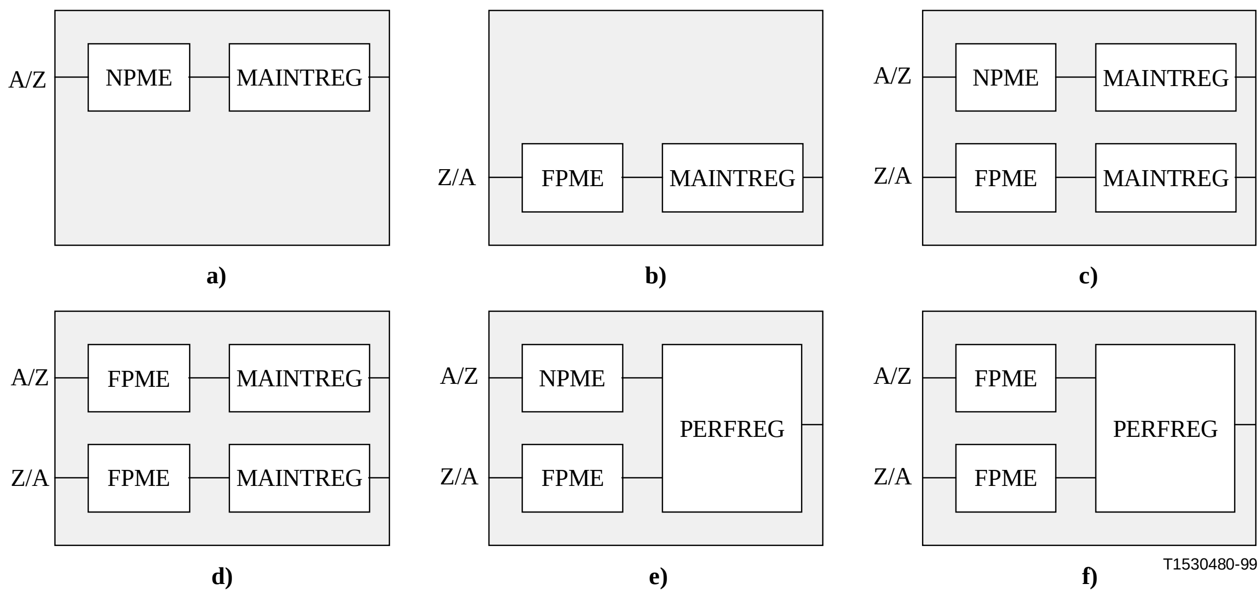
Figure I.1 b) illustrates the performance monitoring process configuration at node Z (head end) supporting a unidirectional (maintenance) application for the single direction (Z-to-A); it uses far-end performance monitoring primitives as input.

Figure I.1 c) illustrates the performance monitoring process configuration at node Z (tail/head end) supporting a unidirectional (maintenance) application for both directions (A-to-Z and Z-to-A); it uses both near-end as well as far-end performance monitoring primitives as input.

Figure I.1 d) illustrates the performance monitoring process configuration at node I (intermediate) supporting a unidirectional (maintenance) application for both directions (A-to-Z and Z-to-A); it uses far-end performance monitoring primitives of both directions as input.

Figure I.1 e) illustrates the performance monitoring process configuration at node Z (tail/head end) supporting the bidirectional (error performance) application; it uses both near-end as well as far-end performance monitoring primitives as input.

Figure I.1 f) illustrates the performance monitoring process configuration at node I (intermediate) supporting the bidirectional (error performance) application; it uses far-end performance monitoring primitives of both directions as input.



A, Z nodes.
A/Z trail in A-to-Z direction.
Z/A trail in Z-to-A direction.

Figure I-1/G.784 – Performance monitoring applications

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems