ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T G.7710/Y.1701 (2020) Amd. 1 (11/2022)

SERIES G: Transmission systems and media, digital systems and networks

Data over Transport – Generic aspects – Transport network control aspects

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Internet protocol aspects – Operation, administration and maintenance

---

Common equipment management function requirements

Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
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
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
General	G.7000–G.7099
Transport network control aspects	**G.7700–G.7799**
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

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

Recommendation ITU-T G.7710/Y.1701

Common equipment management function requirements

Amendment 1

Summary

Recommendation ITU-T G.7710/Y.1701 addresses the equipment management functions (EMFs) inside a transport network element that are common to multiple technologies. For example, common applications are described for date and time, fault management, configuration management, account management, performance management and security management. These applications result in the specification of common EMF functions and their requirements.

The 2019 revision of this Recommendation incorporated the following:

– Recommendation ITU-T G.7710/Y.1701 Amendment 1 (9/2016):

– Create new clause 12 for control plane function management, including fault event reporting for controller-based restoration.

The 2020 revision of this Recommendation has incorporated the following major updates:

– Update clauses 6 and 7 to harmonize with ITU-T G.874, ITU-T G.8051, and ITU-T G.8151;

– Replace the term EMS with MCS;

– Update Figure 3 to use ODUk and packet-based connections for inter-site communications additionally;

– Update Figure 4 for hybrid NE of management network that supports both a media layer and digital layers;

– Update Figures 7 and 62 to replace cZZZ-value with MI_cZZZ;

– Update Figure 22 and clause 8.8 to replace XXX_Reported with ZZZ_Reported to align with ITU-T G.806.

Amendment 1 (Edition 5.1) adds specifications for administrative state management in clause 8.15 and Appendix IV. The numbers of the tables and figures are re-sequenced within each clause of the Recommendation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.7710/Y.1701	2001-11-29	15	11.1002/1000/5635
2.0	ITU-T G.7710/Y.1701	2007-07-29	15	11.1002/1000/9171
2.1	ITU-T G.7710/Y.1701 (2007) Cor.1	2009-11-13	15	11.1002/1000/10419
2.2	ITU-T G.7710/Y.1701 (2007) Amd. 1	2010-07-29	15	11.1002/1000/10894
2.3	ITU-T G.7710/Y.1701 (2007) Cor. 2	2011-04-13	15	11.1002/1000/11134
3.0	ITU-T G.7710/Y.1701	2012-02-13	15	11.1002/1000/11508
3.1	ITU-T G.7710/Y.1701 (2012) Amd. 1	2016-11-13	15	11.1002/1000/13091
4.0	ITU-T G.7710/Y.1701	2019-08-29	15	11.1002/1000/14005
5.0	ITU-T G.7710/Y.1701	2020-10-29	15	11.1002/1000/14503
5.1	ITU-T G.7710/Y.1701 (2020) Amd. 1	2022-11-13	15	11.1002/1000/15144

Keywords

Alarm reporting control, configuration management function, degraded performance, equipment management function, fault management functions, management application function, message communications function, performance management, performance monitoring functions, persistency, severity, thresholding.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 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 expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. 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, ITU had received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.7710/Y.1701

Common equipment management function requirements

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.7710/Y.1701 (2020).

1 Scope

This Recommendation specifies those equipment management function (EMF) requirements that are common to multiple (i.e., two or more) transport technologies (e.g., SDH, OTN, Ethernet, MPLS-TP, MTN, Media). Eventually this Recommendation will include all the common management functions. This Recommendation specifies the capabilities required no matter what technology and where there are differences in requirements for a given feature between technologies, the requirements will be specified in the technology-specific Recommendation. See Appendix I for an overview of common and technology-specific Recommendations. A future version of this Recommendation will elaborate on specific requirements within a given capability.

It must be noted that for a network element (NE) it is not mandatory to support all described applications, and consequently not all specified functions. Depending on the position in the network, the NE may support a subset of the functions. Packages with subsets of these functions can be found in the technology-specific Recommendations.

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; 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.800] Recommendation ITU-T G.800 (2016), *Unified functional architecture of transport networks*.

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[ITU-T G.806] Recommendation ITU-T G.806 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2014), *Generic protection switching – Linear trail and subnetwork protection*.

[ITU-T G.826] Recommendation ITU-T G.826 (2002), *End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections*.

[ITU-T G.827] Recommendation ITU-T G.827 (2003), *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*.

[ITU-T G.828] Recommendation ITU-T G.828 (2000), *Error performance parameters and objectives for international, constant bit-rate synchronous digital paths*.

[ITU-T G.829] Recommendation ITU-T G.829 (2002), *Error performance events for SDH multiplex and regenerator sections*.

[ITU-T G.7702] Recommendation ITU-T G.7702 (2018), *Architecture for SDN control of transport networks*.

[ITU-T G.7712] Recommendation ITU-T G.7712/Y.1703 (2010), *Architecture and specification of data communication network*.

[ITU-T G.8601] Recommendation ITU-T G.8601/Y.1391 (2006), *Architecture of service management in multi-bearer, multi-carrier environment.*

[ITU-T M.20] Recommendation ITU-T M.20 (1992), *Maintenance philosophy for telecommunication networks*.

[ITU-T M.2101] Recommendation ITU-T M.2101 (2003), *Performance limits for bringing-into-service and maintenance of international multi-operator SDH paths and multiplex sections*.

[ITU-T M.2110] Recommendation ITU-T M.2110 (2002), *Bringing into service international multi-operator paths, sections and transmission systems*.

[ITU-T M.2120] Recommendation ITU-T M.2120 (2002), *International multi-operator paths, sections and transmission systems fault detection and localization procedures*.

[ITU-T M.2140] Recommendation ITU-T M.2140 (2000), *Transport network event correlation*.

[ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

[ITU-T M.3013] Recommendation ITU-T M.3013 (2000), *Considerations for a telecommunications management network*.

[ITU-T M.3016.x] Recommendation ITU-T M.3016.x-series (2005), *Security for the management plane*:

Recommendation ITU-T M.3016.0 (2005), *Security for the management plane*: *Overview*.

Recommendation ITU-T M.3016.1 (2005), *Security for the management plane*: *Security requirements*.

Recommendation ITU-T M.3016.2 (2005), *Security for the management plane*: *Security services*.

Recommendation ITU-T M.3016.3 (2005), *Security for the management plane*: *Security mechanism*.

Recommendation ITU-T M.3016.4 (2005), *Security for the management plane*: *Profile proforma*.

[ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (2006), *Principles for the Management of Next Generation Networks*.

[ITU-T M.3100] Recommendation ITU-T M.3100 (2005), *Generic network information model*.

[ITU-T M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions*.

[ITU-T Q.821] Recommendation ITU-T Q.821 (2000), *Stage 2 and stage 3 description for the Q3 interface – Alarm surveillance*.

[ITU-T Q.822] Recommendation ITU-T Q.822 (1994), *Stage 1, stage 2 and stage 3 description for the Q3 interface – Performance management*.

[ITU-T X.700] Recommendation ITU-T X.700 (1992), *Management framework for Open Systems Interconnection (OSI) for CCITT applications*.

[ITU-T X.701] Recommendation ITU-T X.701 (1997), *Information technology – Open Systems Interconnection – Systems management overview*.

[ITU-T X.720] Recommendation ITU-T X.720 (1992), *Information technology – Open Systems Interconnection – Structure of management information: Management information model*.

[ITU-T X.731] Recommendation ITU-T X.731 (1992), *Information technology – Open Systems Interconnection – Systems management: State management function*.

[ITU-T X.733] Recommendation ITU-T X.733 (1992), *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*.

[ITU-T X.734] Recommendation ITU-T X.734 (1992), *Information technology – Open Systems Interconnection – Systems Management: Event report management function*.

[ITU-T X.735] Recommendation ITU-T X.735 (1992), *Information technology – Open Systems Interconnection – Systems Management: Log control function*.

[ITU-T X.744] Recommendation ITU-T X.744 (1996), *Information technology – Open Systems Interconnection – Systems Management: Software management function*.

[ITU-T X.754] Recommendation ITU-T X.754 (2000), *Enhanced Event Control Function*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Terms defined in [ITU-T G.806]:

– atomic function (AF)

– management point (MP).

3.1.2 Terms defined in [ITU-T M.3010]:

– network element (NE)

– network element function (NEF)

– workstation function (WF)

– Q-Interface

– operations system (OS).

3.1.3 Term defined in [ITU-T M.3013]:

– message communication function (MCF).

3.1.4 Term defined in [ITU-T M.3100]:

– management interface.

3.1.5 Term defined in [ITU-T X.700]:

– managed object.

3.1.6 Terms defined in [ITU-T X.701]:

– agent

– manager.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 embedded communication channel (ECC): An ECC provides a logical operations channel between NEs, utilizing, e.g., a data communication channel (DCC) within an SDH or a general communication channel (GCC 0-2) within an OTN as its physical layer.

3.2.2 local craft terminal (LCT): A terminal used for maintenance purposes at the network element (NE).

3.2.3 management application function (MAF): An application process that participates in system management. Each NE and operations system (OS) must support a MAF. A MAF is the origin and termination for all TMN messages.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF	Atomic Function
AIS	Alarm Indication Signal
ALM	Alarm reporting
AP	Access Point
API	Access Point Identifier
AR	Availability Ratio
ARC	Alarm Reporting Control
AST	Alarm Status function
ASY	Alarm Synchronization function
AvFb	Bidirectional Availability Filter function
AvFu	Unidirectional Availability Filter function
BB	Background Block
BBC	Background Block Count
BBE	Background Block Error
BBER	Background Block Error Ratio
BD	Block Delay
BDI	Backward Defect Indication
BDV	Block Delay Variation
BEI	Backward Error Indication
BIS	Bringing-Into-Service
BUT	Begin Unavailable Time
CI	Characteristic Information

CMISE	Common Management Information Service Element
CMSN	Client Management Subnetwork
CP	Connection Point
CPL	Current Problem List function
CPU	Central Processing Unit
CSES	Consecutive Severely Errored Second
CTP	Connection Termination Point
Cur15m-x	Current 15-minute register function (x = c, s, t for Counter, Snapshot and Tidemark)
Cur24h-x	Current 24-hour register function (x = c, s, t for counter, snapshot and tidemark)
DCN	Data Communication Network
DEG	Degraded
DEGM	Degraded Monitor period
DEGTHR	Degraded Threshold
DFE	Decision Feedback Equalizer
DS	Defect Second
EB	Errored Block
EBC	Errored Block Count
EBR	Errored Block Ratio
ECC	Embedded Communication Channel
EDC	Error Detection Code
EMF	Equipment Management Function
EMS	Element Management System
EN	European Norm
ES	Errored Second
ESR	Errored Second Ratio
ETH	Ethernet MAC Layer
EUT	End Unavailable Time
EXE	Excessive
FAS	Frame Alignment Signal
FBBE	Far-end Background Block Error
FCAPS	Fault management, Configuration management, Account management, Performance management and Security management
FD	Frame Delay
FDI	Forward Defect Indication
FDV	Frame Delay Variation
FEC	Forward Error Correction
FE-Mon	Far-End performance Monitor

FES	Far-end Errored Second
FLR	Frame Loss Ratio
FM	Fault Management
FOP	Failure of Protocol
FP	Flow Point
FPME	Far-end Performance Monitoring Event
FSES	Far-end Severely Errored Second
GMT	Greenwich Mean Time
GNE	Gateway Network Element
GPS	Global Positioning System
IAE	Incoming Alignment Error
Id	Identifier
IP	Internet Protocol
LAN	Local Area Network
LB	Lost Block
LBC	Lost Block Count
LBR	Lost Block Ratio
LCN	Local Communication Network
LCT	Local Craft Terminal
LF	Lost Frames
LOC	Loss Of Continuity
LOF	Loss Of Frame
LOG	Event notification Logging function
LOM	Loss Of Multiframe
LOP	Loss Of Pointer
LOS	Loss Of Signal
LTC	Loss of Tandem Connection
MAF	Management Application Function
MCC	Management Communication Channel
MCF	Message Communication Function
MCS	Management and Control System
MD	Mediation Device
MEGID	Maintenance Entity Group Identifier
MEPID	MEG End Point Identifier
MF	Mediation Function
MI	Management Information
MIB	Management Information Base

MIPID	MEG Intermediate Point Identifier
MO	Managed Object
MON	Monitored
MP	Management Point
MSIM	Multiplex Structure Identifier Mismatch
MSP	Multiplex Section Protection
NALM	No Alarm reporting
NBBE	Near-end Background Block Error
NE	Network Element
NEA	Network Element Alarms
NEF	Network Element Function
NEL	Network Element Level
NE-Mon	Near-End performance Monitor
NES	Near-end Errored Second
NGN	Next Generation Network
NMON	Not Monitored
NPME	Near-end Performance Monitoring Event
NSES	Near-end Severely Errored Second
OCh	Optical Channel
OCI	Open Connection Indication
ODI	Outgoing Defect Indication
ODU	Optical Data Unit
OI	Outage Intensity
O.MSN	Optical Management Subnetwork
OMSP	Optical Multiplex Section Protection
OPS	Operational State function
ORF-x	Out of Range Function (x = o, for overflow and u for underflow)
ORR	Out of Range Report
OS	Operations System
OSF	Operations System Function
OTN	Optical Transport Network
PDH	Plesiochronous Digital Hierarchy
PJE	Pointer Justification Event
PLM	Payload Mismatch
PM	Performance Management
PMC	Performance Monitoring Clock
PMF	Performance Monitoring Function

PRBS Pseudo-Random Binary Sequence
PRS Persistency filter
PSC Protection Switch Count
PSE Protection Switch Event
PSL Path Signal Label
QoS Quality of Service
RAS Reliability, Availability and Survivability
RDI Remote Defect Indication
Rec15m-x Recent 15-minute register function (x = c, s, t for Counter, Snapshot and Tidemark)
Rec24h-x Recent 24-hour register function (x = c, s, t for Counter, Snapshot and Tidemark)
REI Remote Error Indication
REP Reportable failure function
RTC Real-Time Clock
RTR Reset Threshold Report
SCC Signalling Communication Channel
SDH Synchronous Digital Hierarchy
SEM Single-Ended Maintenance
SEP Severely Errored Period
SEPI Severely Errored Period Intensity
SES Severely Errored Second
SESR Severely Errored Second Ratio
SEV Severity assignment function
SLA Service Level Agreement
S.MSN SDH Management Subnetwork
SMSN Server Management Subnetwork
SSF Server Signal Fail
STA Station Alarms function
TAN TMN Alarm event Notification function
TBC Transmitted Block Count
TBmin Transmitted Blocks minimum
TCM Tandem Connection Monitoring
TCP Termination Connection Point
TEP TMN Event Pre-processing function
TF Transmitted Frames
TFP Termination Flow Point
ThrF-st standing condition Threshold Function
ThrF-tr transient condition Threshold Function

TI_CK Timer Clock signal

TIM Trace Identifier Mismatch

TMN Telecommunication Management Network

TP Termination Point

TR Threshold Report

TTI Trail Trace Identifier

UAS Unavailable Second

UAT Unavailable Time

UNA Unit Alarms function

UNEQ Unequipped

UTC Coordinated Universal Time

VC Virtual Container

WAN Wide Area Network

WS Workstation

x.MN technology-specific Management Network

x.MSN technology-specific Management Subnetwork

x.NE technology-specific Network Element

5 Conventions

Naming convention for management (sub)networks and network elements:

The general abbreviation for management subnetworks is x.MSN and for management networks it is x.MN. The general abbreviation for network elements is x.NE. The prefix "x." is a placeholder for the various technologies that are managed e.g., "x" could be replaced by:

– "O" meaning an optical management (sub)network or network element.

– "S" meaning SDH management (sub)network or network element.

6 Management architecture

The management of the transport network is based upon a multi-tiered distributed management system as described in [ITU-T M.3010] and based on an NGN management architecture as described in [ITU-T M.3060]. Each tier provides a predefined level of network management capabilities. The lowest tier of this organizational model, illustrated in Figure 6-1, includes the network element functions (NEFs) that provide the transport service and the operations system functions (OSFs) at the element management level. The management application function (MAF) within the NEFs and OSFs provides the management support. 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.

The management communication to peer NEFs and/or operations system functions (OSFs) is provided via the message communication function (MCF) within each entity (NEF, OSF). The user can access the management of the transport network via a local craft terminal (LCT) attached to the NEF or via a workstation (WS) attached to the OSF.

The specification of the MAF and the MCF in the NEF is within the scope of this Recommendation.

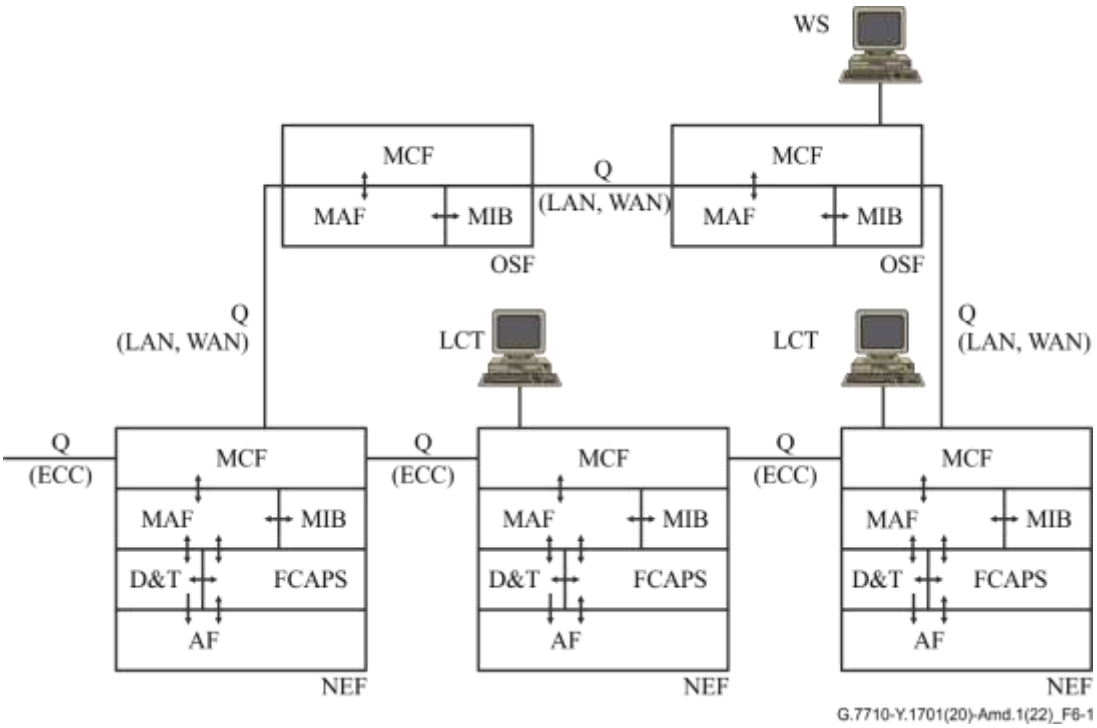


Figure 6-1 – Management organizational model

The embedded communication channel (ECC) provides a logical operations channel between NEs for transferring management and/or signalling information. Note that some technologies provide separate communication channels for management (MCC) and signalling (SCC). Whenever the generic term ECC is used in this Recommendation, it mainly focuses on the utilization of the ECC for management (i.e., MCC only).

The local craft terminal (LCT) and its interface to the NEF, shown in Figure 6-1, are not within the scope of this Recommendation.

6.1 Management network architecture

6.1.1 Relationship between TMN, x.MN and x.MSN

The telecommunication management network (TMN) may consist of several technology-specific management networks (x.MN), which in turn may be partitioned into management subnetworks (x.MSN). An example of these relationships is shown in Figure 6-2 for an optical management network, an SDH management network, and another (x) management network.

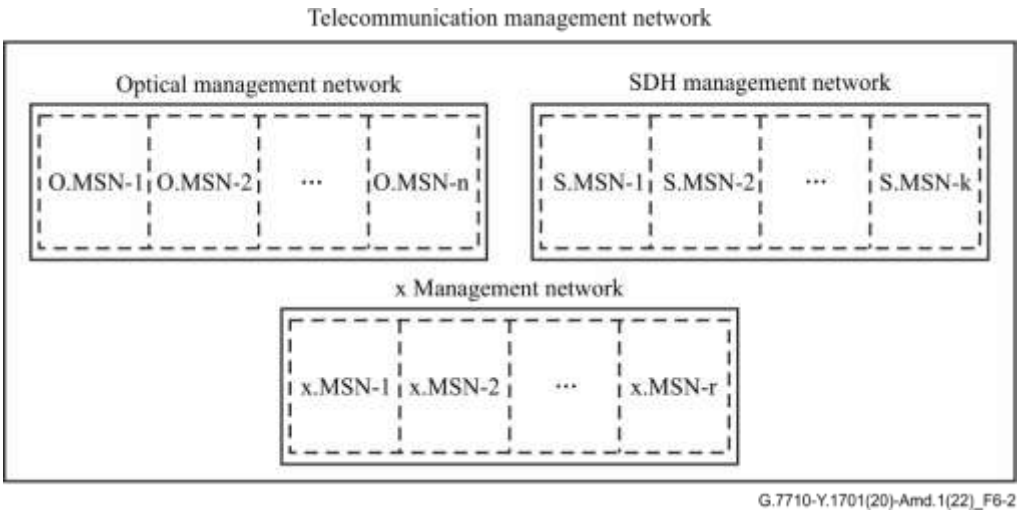


Figure 6-2 – TMN, x.MN and x.MSN partitioning

Figure 6-3 shows an example of a management network and its integration into the telecommunication management network (TMN). The data communication network (DCN) between these physical blocks is defined in [ITU-T G.7712].

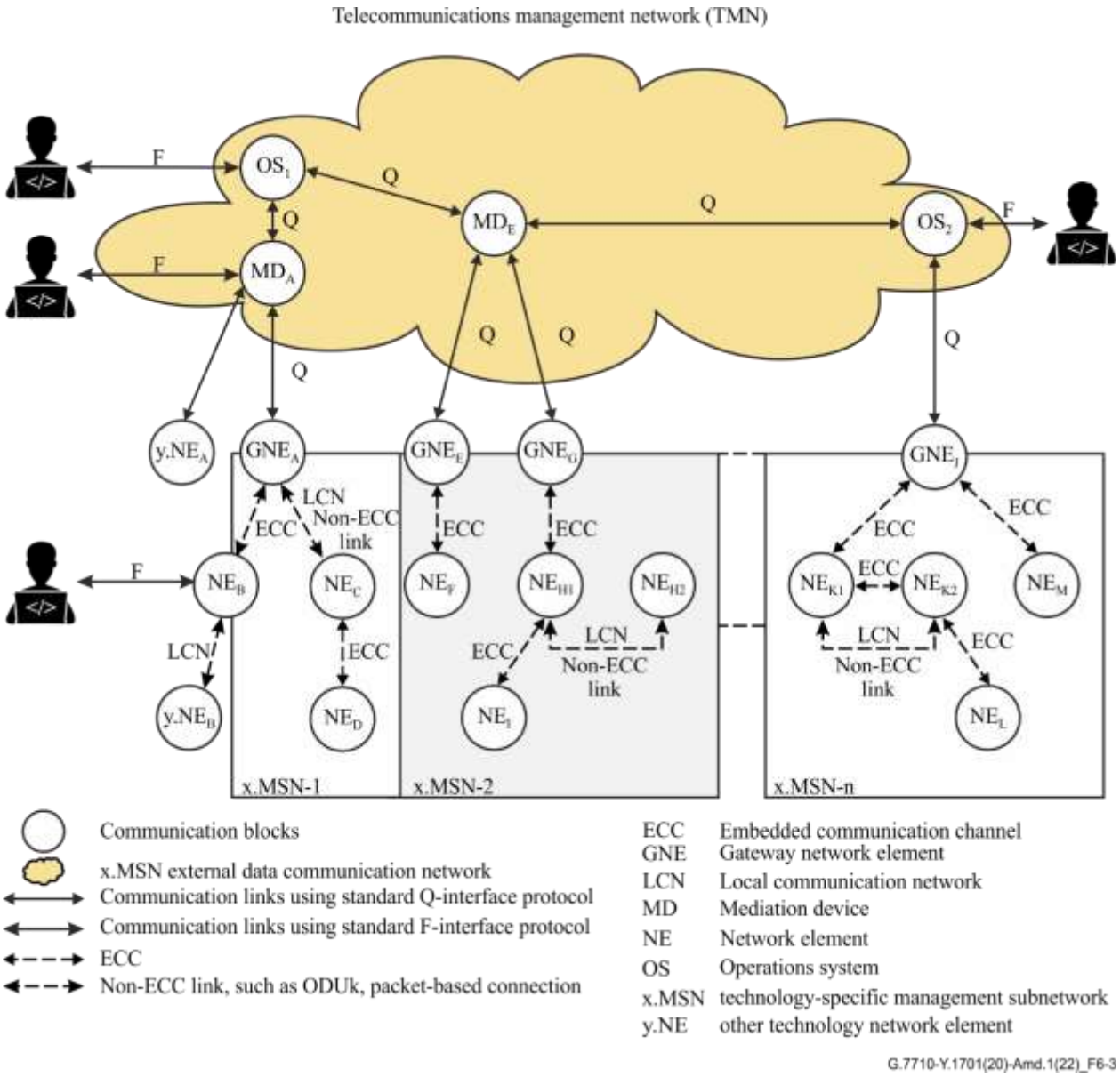


Figure 6-3 – Management network example

NEs must support management communications functions. The MCF of an NE initiates or terminates (in the sense of the lower protocol layers), forwards, or otherwise processes management messages over ECCs, or over other DCN interfaces.

6.1.2 Access to the x.MSN

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

– Local craft terminal;

– Mediation device (Q-interface);

– Operations system interfaces (Q-interface).

The functionality required to be supported by the NE will determine the type of Q-interface to be provided. For instance, the two main varieties of NEs expected are the NEs with mediation functions (MF) and "regular" NEs.

6.1.3 x.MSN requirements

In Figure 6-3, a number of requirements should be noted concerning the architecture of the x.MSN:

a) *Multiple NEs at a single site*

Multiple, addressable NEs may be present at a single physical location. For example, in Figure 6-3, NE_E and NE_G may be collocated at a single equipment site.

b) *NEs and their communications functions*

The message communication function of an NE initiates/terminates (in the sense of the lower protocol layers), routes, or otherwise processes management messages over ECCs, or other data communication network interfaces connected via an external Q-interface.

c) *Inter-site communications*

The inter-site or inter-office communications link between the NEs will normally be provided by the ECCs. Ethernet WAN can also be used to carry communications that require a higher throughput or a lower latency than those that could be provided by the ECCs.

d) *Intra-site communications*

Within a particular site, the NEs may communicate via an intra-site ECC or via an Ethernet LAN. Figure 6-3 illustrates both instances of this interface.

All the NEs are required to either terminate an Ethernet LAN (for intra site communication with a co located NE) or an ECC. In addition, the NE may also be required to support other DCN interfaces.

6.1.4 x.MSN data communication network

It is intended that this Recommendation should place no restriction on the physical transport topology to support management communications. Thus, it is expected that the supporting data communication network (DCN) may contain string (bus), star, ring or mesh topologies. The DCN also supports seamless connectivity with remote transport domains and NEs as specified in [ITU-T G.8601] as well as with termination points located in NEs under control by a third-party network operator as specified in [ITU-T G.8601].

See [ITU-T G.7712] for the management of DCN's architectures and specifications, including the network layer protocol.

Each management subnetwork (x.MSN) must have at least one NE which is connected to an OS (possibly via a mediation device). This NE is called a gateway network element (GNE) and is illustrated in Figure 6-3. The GNE should be able to perform an intermediate system network layer routing function for DCN messages destined for any end system in the x.MSN. Messages passing between the OS and any of the end systems in the subnetwork are routed through the GNE and, in general, other intermediate systems.

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

The other NEs within the management subnetwork (x.MSN) must, at least, be able to perform an end system network layer function to terminate the DCN messages destined to itself. They may also be able to perform an intermediate system network layer routing function for DCN messages destined to any other end system in the x.MSN or to the OS.

6.1.5 Management of the DCN

NEs communicate via the DCN. In order to have the DCN operate properly, a number of management functions are required, including:

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

2) establishment of message routing between DCN nodes

3) management of DCN network addresses

4) retrieval of operational status of the DCN service at a given node

5) capability to enable/disable access to the DCN (if supporting a management protocol);

6) get the topology view of the DCN.

6.1.6 Remote log-in

For remote log-in security, see requirements in [ITU-T M.3016.x].

6.1.7 Relationship between technology domains

The transport network has to deal with many technology domains (i.e., connection-oriented and connectionless). When they are connected together, these domains create a client-server relationship between them. This situation leads to *hybrid* NEs that handle a specific technology internally and in the transport ports, but also have access ports, which are able to convert from another technology to this specific one.

Figure 6-4 shows such a client-server relationship between two different management subnetworks. Figure 6-4(a) exemplifies the case that the two subnetworks are different digital network technologies. NEs C and D contain technology B (server) layer network entities and technology A (client) layer network entities. These NEs are therefore part of more than one type of management subnetwork. The technology A ports in NEs C and D can be managed in one of the following ways:

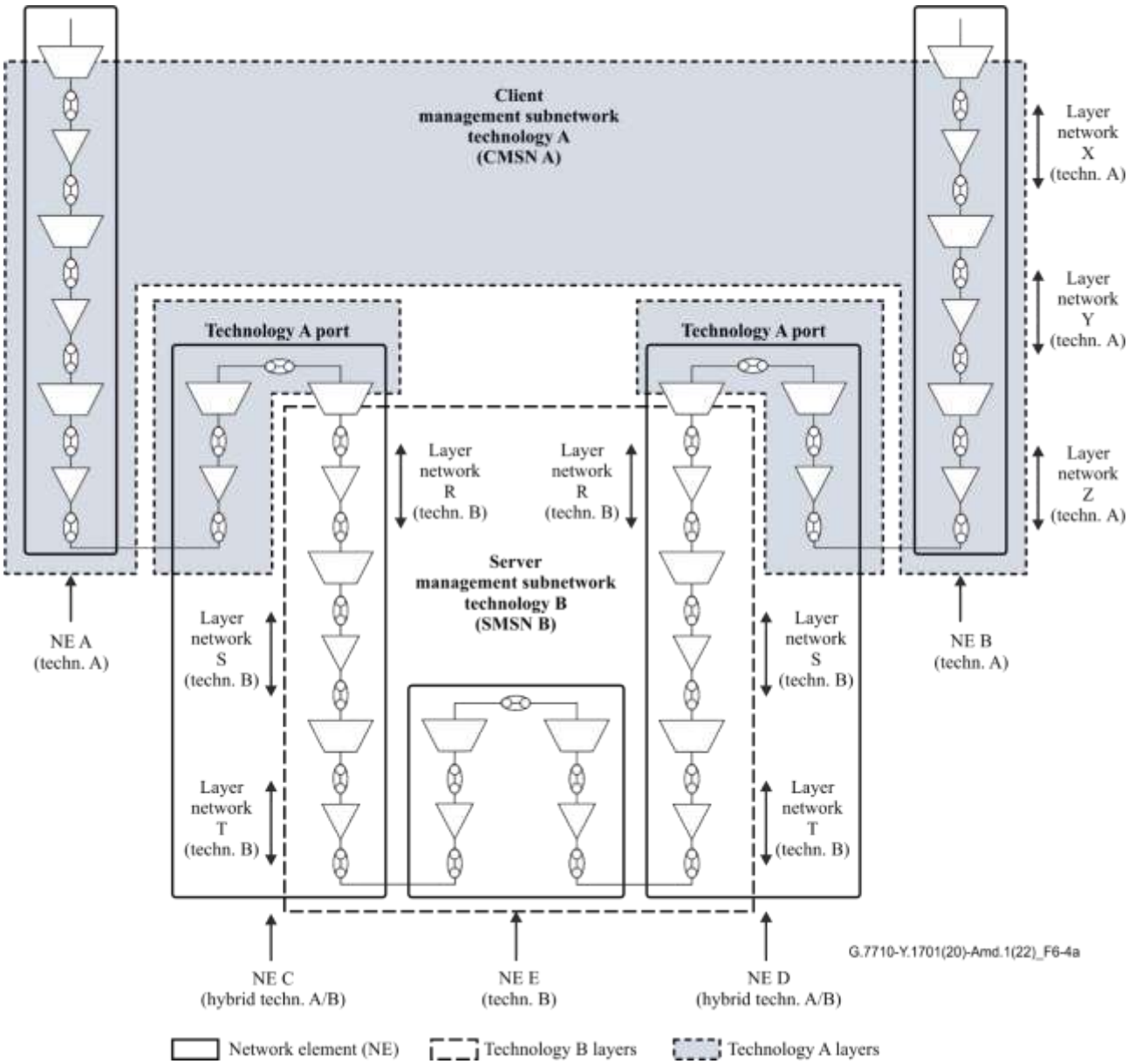
– as an entity that is managed by the CMSN OSF;

– as an entity that is managed by the SMSN OSF;

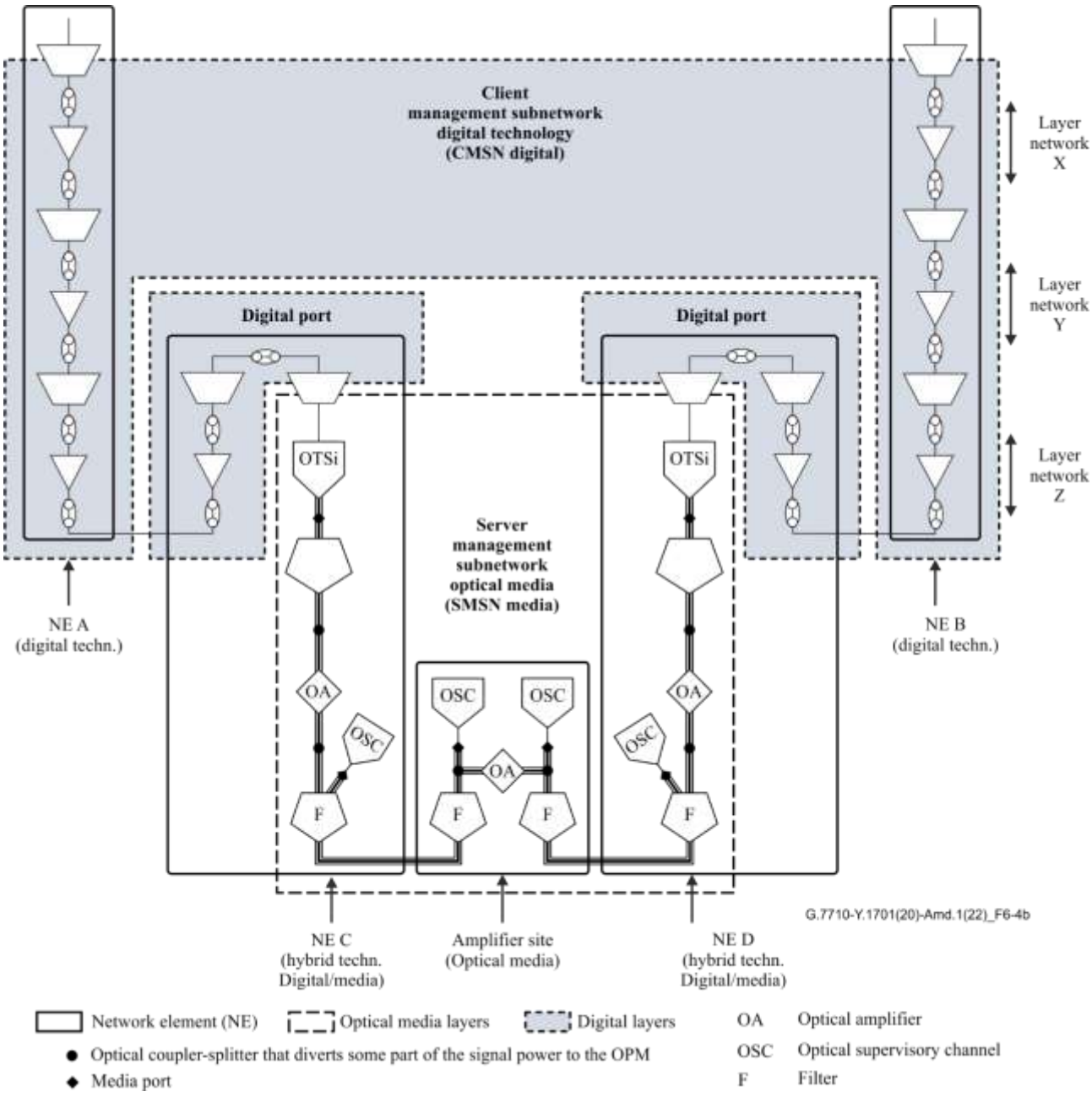
– as a stand-alone fragment which is not managed except as an equipment fragment.

This may be achieved by one or more agents within such an NE, using one or more protocols to communicate with their respective OSFs. In this example, there is a separate OSF (one for the CMSN and one for the OMSN) for each domain, which may or may not be collocated in the same physical OS.

Figure 6-4(b) exemplifies the case that two subnetworks are digital and media network technologies. The technology digital ports in NEs C and D can be managed in one of the three ways above.


Client
management subnetwork
technology A
(CMSN A)
Layer
network
X
(techn. A)
Layer
network
Y
(techn. A)
Layer
network
Z
(techn. A)
Technology A port
Technology A port
Layer
network
R
(techn. B)
Layer
network
R
(techn. B)
Server
management subnetwork
technology B
(SMSN B)
NE A
(techn. A)
Layer
network
S
(techn. B)
Layer
network
S
(techn. B)
NE B
(techn. A)
Layer
network
T
(techn. B)
Layer
network
T
(techn. B)
G.7710-Y.1701(20)-Amd.1(22)_F6-4a
NE C
(hybrid techn. A/B)
NE E
(techn. B)
NE D
(hybrid techn. A/B)
Network element (NE)
Technology B layers
Technology A layers

(a)



(b)

Figure 6-4 – Example of management network relationships, (a) digital to digital subnetworks, (b) digital to media subnetworks

6.2 Equipment management architecture

This clause provides an overview of the minimum functions that are required to support inter vendor NE management including single-ended maintenance of NEs within an x.MSN or between communicating peer NEs across a network interface. Single-ended maintenance is the ability to access remotely located NEs to perform maintenance functions (see clause 10 for the performance management applications).

It should be noted that the management functions have been categorized according to the classifications given in [ITU-T X.700].

The equipment management function (EMF) provides the means through which a management and control system (MCS), such as an element management system (EMS), an SDN controller, and other managing entities, manage the network element function (NEF). Figure 6-5 illustrates the EMF

components within the network element (NE). It must be noted that this illustration does not provide an exhaustive description of the functions that may be contained in an NEF (e.g., within atomic functions, EMF, MCF). If an NE contains an internal manager, this manager will be part of the EMF.

The EMF interacts with the transport and synchronization layer atomic functions (AF) by exchanging management information (MI) across the management point (MP) reference points. See [ITU-T G.806] for more information on atomic functions and reference points. The EMF contains a number of functions that provide a data reduction mechanism on the information received across the MP reference points.

The EMF includes functions such as date and time and the FCAPS (fault, configuration, accounting, performance and security) functions. The EMF contains a number of functions that provide a data reduction mechanism on the information received across the MP reference points. The outputs of these functions are available to the agent via the NE resources and MAFs that represent this information as managed objects. See Figure 6-5. The EMF provides event message processing, data storage and logging. The MAF processes the information provided to and by the NE resources. The agent converts internal MI signals into management application messages and vice versa. The agent responds to management application messages from the message communication function (MCF) by performing the appropriate operations on the managed objects in a management information base (MIB) (see [ITU-T X.701] and [ITU-T X.720] for more information on managed objects), as necessary. The MCF contains communications functions related to the outside world of the NEF (i.e., date and time, management plane (management via EMS), control plane (management via ASON connection controller), local craft terminal (management by user) and local alarms).

The date and time functions keep track of the NE's date and time. The FCAPS functions that need date and time information, e.g., to time-stamp event reports, get this information from the date and time functions.

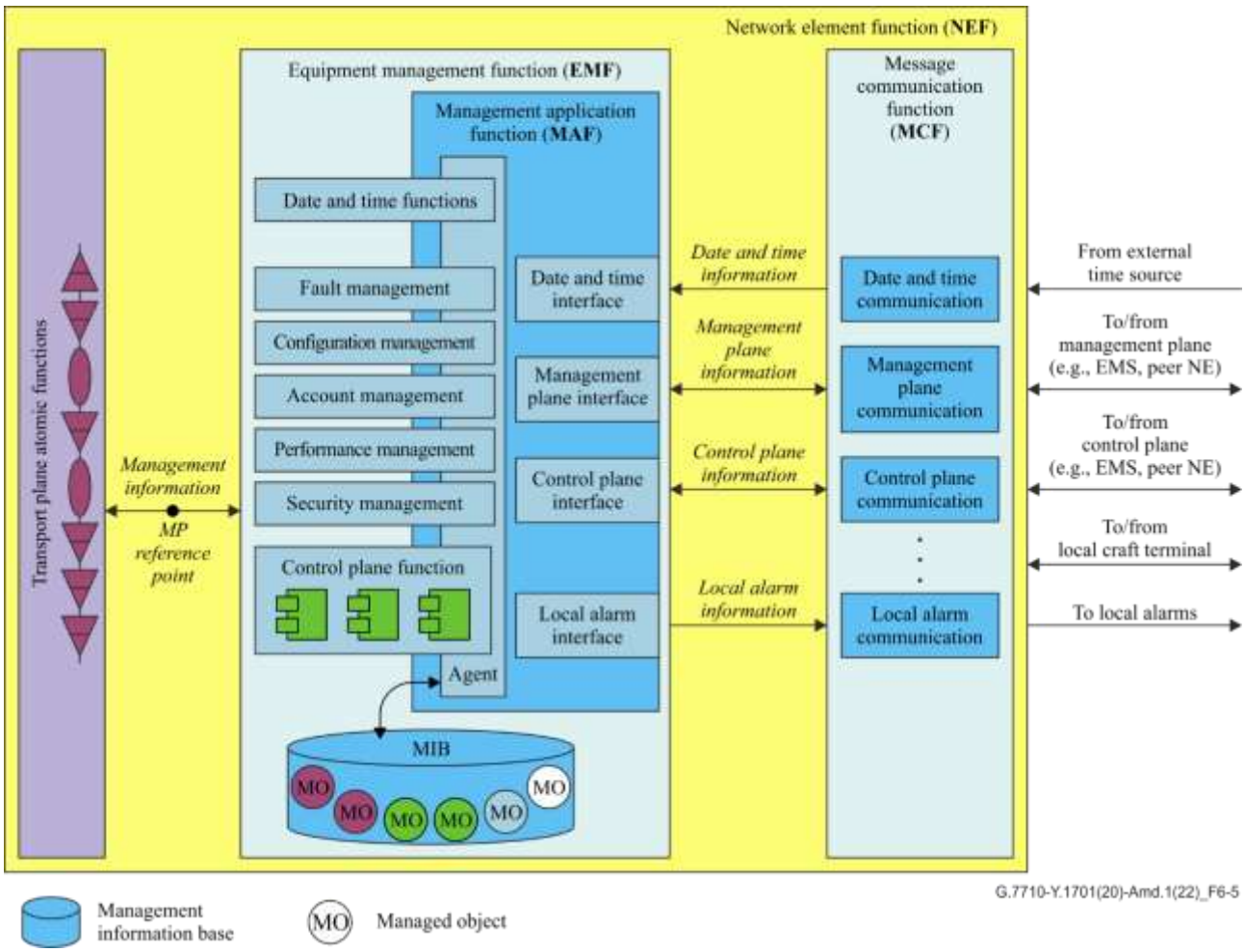


Figure 6-5 – Equipment management function process block diagram

This Recommendation focuses on the EMF functions that affect the MI flows, originate the MI flows, or receive the MI flows.

6.2.1 Management information base (MIB)

All managed object instances within an NE shall be stored in a management information base (MIB). The following functions are required regarding the MIB:

1) *Get MIB of NE*:

   This function allows the OS to get the list of all object instances stored in the MIB of the NE. The list contains the objects and their relationships, i.e., connectivity pointers and containment relations (name binding). The function should be used by the OS to maintain its NEL-OS database. It is generally used for an NEL-OS database initialization at the network installation phase, or for a database recovery due to a discrepancy with the NE MIB after a network upgrade.

2) *Report NE MIB changes to the OS*:

   This function reports a new resource to the OS when it is inserted in the equipment, or to dismiss an entity when it is removed. When the hardware in the NE is changed by adding or removing a resource (e.g., port, card), the MIB in the OS has to be updated.

   The removing of a resource from an NE, and the deletion of the affected managed object instances shall be reported to the OS.

6.3 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 of a NE is described in specific detail for each atomic function in the technology specific NE equipment Recommendations.

The information flow over the MP reference points that arises from provisioning and reporting data is described in specific detail for each atomic function in the technology specific NE equipment Recommendations.

The input information across an MP refers to the provisioning data that is passed from the EMF to the atomic functions. The output information across an MP refers to the reports passed to the EMF from the atomic functions.

7 Fault management

Fault management is a set of functions, which enables the detection, isolation and correction of abnormal operation of the telecommunication network and its environment. It provides facilities for the performance of the maintenance phases from [ITU-T M.20]. The quality assurance measurements for fault management include component measurements for reliability, availability and survivability (RAS).

The requirements for the fault management functions are specified in clause 7.2. These requirements are based on the fault management applications, described in clause 7.1.

7.1 Fault management applications

The six basic fault management applications according to [ITU-T M.3400] are:

– *RAS quality assurance*

  RAS quality assurance establishes the reliability criteria that guides the design policy for redundant equipment (a responsibility of configuration management), and the policies of the other function groups in this area.

– *Alarm surveillance*

  A TMN provides the capability to monitor NE failures in near-real time. When such a failure occurs, an indication is made available by the NE. Based on this, a TMN determines the nature and severity of the fault. For example, it may determine the effect of the fault on the services supported by the faulty equipment. This can be accomplished in either of two ways: a database within a TMN may serve to interpret binary alarm indications from the NE, or if the NE has sufficient intelligence, it may transmit self-explanatory messages to a TMN. The first method requires little of the NE beyond a basic self-monitoring capability. The second method requires additionally that both the NE and a TMN support some type of message syntax that will allow the adequate description of fault conditions.

  Alarm information can be reported at the time of occurrence, and/or logged for future access. An alarm may also cause further management actions within the NE that lead to the generation of other fault management data.

– *Fault localization*

  Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines. The routines can employ internal or external test systems and can be controlled by a TMN (see [ITU-T M.20]).

– *Fault correction*

  Fault correction transfers data concerning the repair of a fault and for the control of procedures that use redundant resources to replace equipment or facilities that have failed.

– *Testing*

  Testing can be carried out in one of two ways. In one case, a TMN directs a given NE to carry out analysis of circuit or equipment characteristics. Processing is executed entirely within the NE and the results are automatically reported to the TMN, either immediately or on a delayed basis.

  Another method is where the analysis is carried out within the TMN. In this case, the TMN merely requests that the NE provide access to the circuit or equipment of interest and no other messages are exchanged with the NE.

– *Trouble administration*

  Trouble administration transfers trouble reports originated by customers and trouble tickets originated by proactive failure detection checks. It supports action to investigate and clear the trouble and provides access to the status of services and the progress in clearing each trouble.

Within the scope of this Recommendation, i.e., the equipment management functions inside the NE, the applications are limited to alarm surveillance. The alarms are gathered, pre-processed and partly analysed in the NE for the purpose of maintenance, bringing-into-service, quality of service, reporting and thresholding.

The following subclauses specify the applications necessary for alarm surveillance for transport network elements.

7.1.1 Supervision

The supervision process describes the way in which the actual occurrence of a disturbance or fault is analysed with the purpose of providing an appropriate indication of performance and/or detected fault condition to maintenance personnel. The supervision philosophy is based on the concepts underlying the architectural model of [ITU-T G.800] (for unified functional architecture of transport network), [ITU-T G.807] (for media layer networks) and [ITU-T G.805] (for connection-oriented networks), and the alarm reporting function of [ITU-T X.733].

The five basic supervision categories are related to transmission, quality of service, processing, equipment and environment. These supervision processes are able to declare fault causes, which need further validation before the appropriate alarm is reported.

The NE shall indicate to the OS when a TP is no longer able to supervise the signal (e.g., implementing equipment has a fault or loss of power).

7.1.1.1 Transmission supervision

Transmission supervision processes are concerned with the management of the transmission resources in the network and they are only interested in the functionality that is being provided by an NE. It requires a functional representation of an NE that is implementation independent.

Most functions process the signals to detect the occurrence of certain characteristics and provide performance information or alarm conditions based on these characteristics. Therefore, transmission supervision processing provides information on the external interface signals that are processed by an NE.

Transmission supervision comprises:

– Continuity supervision for the detection of a broken connection, e.g., a cable cut or open matrix. This condition is determined by the sink function at the arrival of "no signal" (LOS), the "unequipped indication" (UNEQ) or the "open connection indication" (OCI). In case of an open matrix, the source function sends the UNEQ or OCI indication.

– Connectivity supervision for the detection of a misconnection, e.g., a misconnected cable or an incorrect matrix connection. This condition is determined by the sink function at the arrival of an unexpected value of the trail trace identifier (trace identifier mismatch (TIM)). The source function sends the agreed TTI value.

– Signal quality supervision for the detection of degraded performance (DEG). This condition is determined by the sink function, e.g., based on the calculation of the error detection code (EDC) violations. The source function sends the EDC.

– Payload type supervision for the detection of incompatible adaptation functions at the ends of trails, e.g., the source uses bit synchronous mapping while the sink expects byte synchronous mapping. This condition is determined by the sink function at the arrival of an unexpected value of the path signal label (payload type mismatch (PLM)). The source function sends the PSL value that corresponds with the mapping.

– Multiplex structure supervision for the detection of a wrong payload structure.

– Alignment supervision for the detection of wrong frame alignment, i.e., the receiving end considers the start of the frame at the wrong position. This condition is determined by the sink function at the arrival of a wrong frame alignment signal (loss of frame (LOF); loss of multiframe (LOM)) at the considered frame start position. The source function sends the FAS at a specified position in the frame.

– Protocol supervision for the detection of failures in the sequence of a protocol exchange, e.g., a failure in the automatic protection switching protocol. This condition is determined by the sink function at the arrival of an unexpected (i.e., out of sequence) protocol message, after which the sink function declares a failure of protocol (FOP) defect.

– Single ended supervision to be able to monitor the trail status in both directions at a single location, e.g., to monitor the occurrence of defects, detected at both ends of the trail. These occurrences (backward failures) are monitored at the trail termination or connection points by reading the remote defect indication (RDI) or backward defect indication (BDI). The source function sends the RDI or BDI.

– Alarm suppression is considered as part of the transmission supervision process. Its aim is not only to alarm the root cause, but also to suppress resulting alarms in the detecting NE and all downstream NEs. This condition (forward failure) is determined by the sink functions at the arrival of an alarm indication signal (AIS) or forward defect indication (FDI). The source function sends the AIS or FDI.

NOTE 1 – A misconnection due to an open matrix could be detected by the continuity supervision process, rather than by the connectivity supervision process.

NOTE 2 – An inconsistent payload structure or inconsistent payload type could be detected by the alignment supervision process, rather than by the multiplex supervision process or the payload type supervision process.

Transmission failures can be subdivided between primary failures and secondary/consequential failures. Primary failures, in general, indicate the cause of the fault, e.g., a broken cable or a misconnection. The primary failure reports indicate the fault location and initiate a repair action. Secondary or consequential failures, in general, indicate whether the service is up or down. They are generated to suppress alarms, e.g., AIS, SSF, FDI.

Transmission failures can be associated with the three types of transport atomic functions: termination, adaptation and connection. Table 7-1 gives examples.

Table 7-1 – Atomic function associated transmission failure list

	Termination sink	Adaptation sink	Connection
Primary failures	Continuity failure, e.g., loss of signal (LOS), loss of continuity (LOC), unequipped (UNEQ), open connection indication (OCI).	Framing failure, e.g., loss of frame (LOF), loss of multiframe (LOM), loss of pointer (LOP).	Protocol failure, e.g., failure of protocol (FOP).
	Connectivity failure, e.g., trace identifier mismatch (TIM).	Payload type failure, e.g., payload mismatch (PLM).	
	Degradation failure, e.g., signal degraded (DEG).	Payload structure failure, e.g., multiplex structure identifier mismatch (MSIM).	
	Connection monitoring source failure, e.g., loss of tandem connection (LTC).		
Secondary or consequential failures	Forward failure, e.g., alarm indication signal (AIS), forward defect indication (FDI), server signal fail (SSF).	Forward failure, e.g., alarm indication signal (AIS), forward defect indication (FDI), server signal fail (SSF).	
	Backward failure, e.g., backward/remote/outgoing defect indication (BDI/RDI/ODI).		

Details of transmission supervision are described in clause 6 of [ITU-T G.806].

7.1.1.2 Quality of service supervision

Quality of service supervision is principally associated with degradation in the performance. Annex A of [ITU-T X.733] lists the following probable causes in this category: excessive response time, exceeded queue size, reduced bandwidth, excessive retransmission rate, threshold crossed, degraded performance, congestion, resource at or nearing capacity. This Recommendation elaborates on degraded performance and threshold crossings only. Note that signal quality supervision is, for historical reasons, part of transmission supervision.

7.1.1.3 Processing supervision

Processing supervision is principally associated with a software or software processing fault. Annex A of [ITU-T X.733] lists the following probable causes in this category: storage capacity problem, version mismatch, corrupt data, CPU cycles limit exceeded, software error, software program error, software program abnormally terminated, file error, out of memory, underlying resource unavailable, application subsystem failure, configuration of customization error. As these probable causes are implementation-specific and vendor-specific, they are not subject to standardization. Note that protocol supervision is, for historical reasons, part of transmission supervision.

7.1.1.4 Hardware supervision

Equipment supervision processing is concerned with the fault localization and repair of the equipment itself. Its purpose is to answer the classic questions: "who to send where to repair what?" It does not require knowledge of the transmission network. Annex A of [ITU-T X.733] lists the following probable causes in this category: power problem, timing problem, processor problem, dataset or modem error, multiplexer problem, receiver or transmitter failure, input-output device error,

equipment malfunction, adapter error. In general, within the scope of this Recommendation, equipment supervision comprises the supervision of interchangeable and non-interchangeable units and cables. As these probable causes are implementation-specific and vendor-specific, they are not subject to standardization.

7.1.1.5 Environmental supervision

Environmental supervision is principally associated with a condition related to ambient conditions within an enclosure in which the equipment resides. Annex A of [ITU-T X.733] lists the following probable causes in this category: temperature unacceptable, humidity unacceptable, heating/ventilation/cooling system problem, enclosure door open, pump failure, etc. In general, within the scope of this Recommendation, environmental supervision comprises the supervision of sensor contacts, known as miscellaneous discrete inputs. As these probable causes are implementation-specific and vendor-specific, they are not subject to standardization.

7.1.2 Validation

A fault cause indicates a limited interruption of the required function. A fault cause is not reported to maintenance personnel because it could exist for a very short time only. Some of these events however are summed up in the performance monitoring process, and when this sum exceeds a certain value, a threshold report can be generated (see clause 10.1.7).

When the fault cause lasts long enough, an inability to perform the required function arises. This failure condition is subject to be alarmed to maintenance personnel because corrective action might be required. Conversely, when the fault cause ceases to be declared after a certain time, the failure condition must disappear.

Validation is concerned with the integration of fault causes into failures. As this integration is only time-based, the related function is called fault cause persistency (see clause 7.2.1).

7.1.3 Alarm handling

7.1.3.1 Severity assignment

Failures may have been categorized to indicate the severity or urgency of the fault. [ITU-T M.20] and [ITU-T X.733] define different, though comparable categories. [ITU-T M.3100] has extended the [ITU-T X.733] list. Table 7-2 summarizes these categories.

Table 7-2 – Severity categories

M.20	X.733	M.3100	Description
Prompt maintenance alarm	Critical	Critical	Indication for a service-affecting condition. Immediate corrective action is required.
	Major	Major	Indication for a service-affecting condition. Urgent corrective action is required.
Deferred maintenance alarm	Minor	Minor	Indication for a non-service-affecting condition. Corrective action should be taken in order to prevent more serious fault.
Maintenance event information	Warning	Warning	Indication for a potential or impending service-affecting fault. Further diagnosis should be made.
–	–	Not alarmed	Indication to indefinitely suppress reporting.

NOTE 1 – The severities "cleared" and "indeterminate" defined by [ITU-T X.733] are not included in Table 7-2, as it is assumed that these are not to be used to assign a failure.

NOTE 2 – The severities, defined by [ITU-T M.20], are mainly used for presentation by LEDs. The severities, defined by [ITU-T X.733] reflect the underlying management messages.

For maintenance personnel, it is important to know the urgency of the required action. The severity assignment function (see clause 7.2.2) has the capability to assign a severity to a failure.

The severity "Not alarmed" suppresses the reporting of a failure per managed entity and per event or failure type.

The severity for each failure instance may be provisioned to a value other than the default. For example, when no trail trace identifiers are used in the network, the primary failure TIM may be provisioned to "Not alarmed". Another example is to provision the secondary failure AIS to "Critical" at the ingress of the network. In this way, the operator is aware of whether or not the customer signal carries traffic.

7.1.3.2 Alarm reporting control

The following alarm reporting control (ARC) states may be specified for a managed entity:

ALM Alarm reporting; alarm reporting is turned on.

NALM No alarm reporting; alarm reporting is turned off.

NALM-CD No alarm reporting, countdown; this is a sub-state of NALM-QI and performs the persistence timing countdown function when the managed entity is qualified problem free.

NALM-NR No alarm reporting, not ready; this is a sub-state of NALM-QI and performs a wait function until the managed entity is qualified problem free.

NALM-QI No alarm reporting, qualified inhibit; alarm reporting is turned off until the managed entity is qualified problem free for a specified persistence interval.

NALM-TI No alarm reporting, timed inhibit; alarm reporting is turned off for a specified timed interval.

ARC supports an automatic in-service provisioning capability. Alarm reporting may be turned off (using NALM, NALM-TI, or NALM-QI) on a per managed entity basis to allow sufficient time for customer service testing and other maintenance activities in an "alarm free" state. Once a managed entity is ready, alarm reporting is automatically turned on (to ALM). The managed entity may be automatically turned on either by using NALM-TI or NALM-QI and allowing the resource to transition out automatically, or by invoking first the NALM state from an EMS and, when maintenance activity is done, invoking the ALM state. This later automation is carried out by the EMS. For further details relating to ARC, see [ITU-T M.3100].

It is critical during maintenance activities that alarm monitoring of the managed entity continues to occur. By maintaining managed entity monitoring, technicians can retrieve alarm and performance information to troubleshoot during the provisioning or maintenance process, or later during a post-mortem on a provisioning task gone awry. ARC addresses this need.

ARC includes a persistence interval before reporting begins in recognition of the fact that during provisioning and during customer turn-up activities, the managed entity may become available briefly, only to be lost again as the service configuration is changed.

ARC applies to all managed entities that provide alarm reporting and especially to all managed resources autonomously provisioned by the managed system/managed application, and all managed entities that may be pre-provisioned via a management interface.

By activating alarm reporting control, the technicians and OS systems will not be flooded with unnecessary work items during operations activities such as service activation and the customer's service turn-up activities. This will reduce maintenance costs and improve the operation and maintenance of these systems.

7.1.3.3 Reportable failures

Figure ~~6~~7-1 outlines a managed entity with its associated failures. In this general case, the managed entity, e.g., a termination sink function, can declare a number of primary and secondary failures. The reporting of these failures is controlled by two report options. The first option, alarm severity assignment, when "Not alarmed" indefinitely suppresses reporting for that failure. The second option, alarm reporting control (ARC), temporarily controls the reporting of the failure by means of the ARC mode.

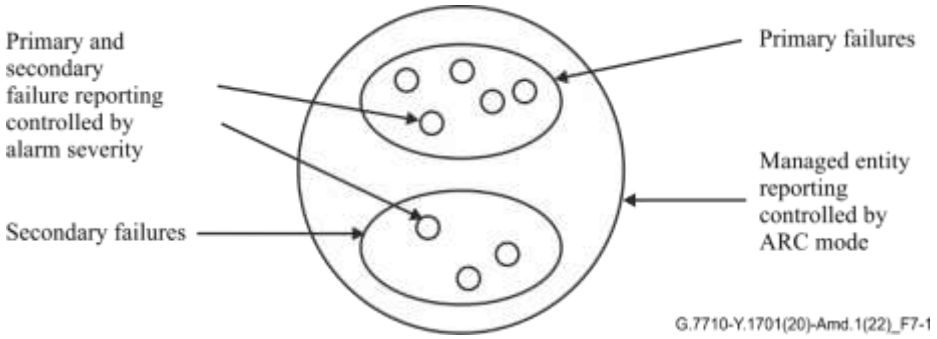


Figure ~~6~~7-1 – Managed entity with associated failures

7.1.3.4 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 NE shall have the ability to accept OS directions related to which events and conditions generate autonomous reports and which shall be reported on request.

The following alarm-related functions shall be supported:

1) autonomous reporting of alarms;
2) request for reporting of all alarms;
3) reporting of all alarms;
4) allowance or inhibition of autonomous alarm reporting;
5) reporting on request status of allow or inhibit alarm reporting;
6) control of the trail termination point mode and port mode;

NOTE – Applicable only to SDH and PDH and superseded for new development (e.g., OTN). See Appendix III.

7) reporting of protection switch events.

7.1.3.4.1 Local reporting

Local reporting is concerned with alarming by means of audible and visual indicators near the failed equipment. These bells and lamps could be organized in a certain hierarchy, so that maintenance personnel are able to follow the trail of lights (or bells) to locate the failed equipment. Based on the indicator value (e.g., the sound, the colour and flashing of the light, the message on a display), maintenance personnel are able to execute the appropriate corrective action.

Local reports include:

– unit alarms;
– network element alarms;
– station alarms.

7.1.3.4.2 TMN reporting

TMN reporting is concerned with reporting to an OS. These reports are either autonomous reports (notifications) or reports on request by maintenance personnel.

TMN reports include:

– TMN alarm event notifications
– alarm log
– alarm synchronization
– current problem list
– alarm status
– operational state.

7.2 Fault management functions

Figure 7-2 contains a functional model of fault management inside the EMF. This model is consistent with the alarm flow functional model, specified in [ITU-T M.3100]. It must be noted that this figure does not address configuration aspects relating to fault management, the full ARC functional model, nor does it define where all possible event report parameters get assigned. This figure is only intended to illustrate which well-known functions are impacted by ARC and which are not, and to provide a generalized alarm flow view.

Specifications of the functions are given in subsequent clauses.

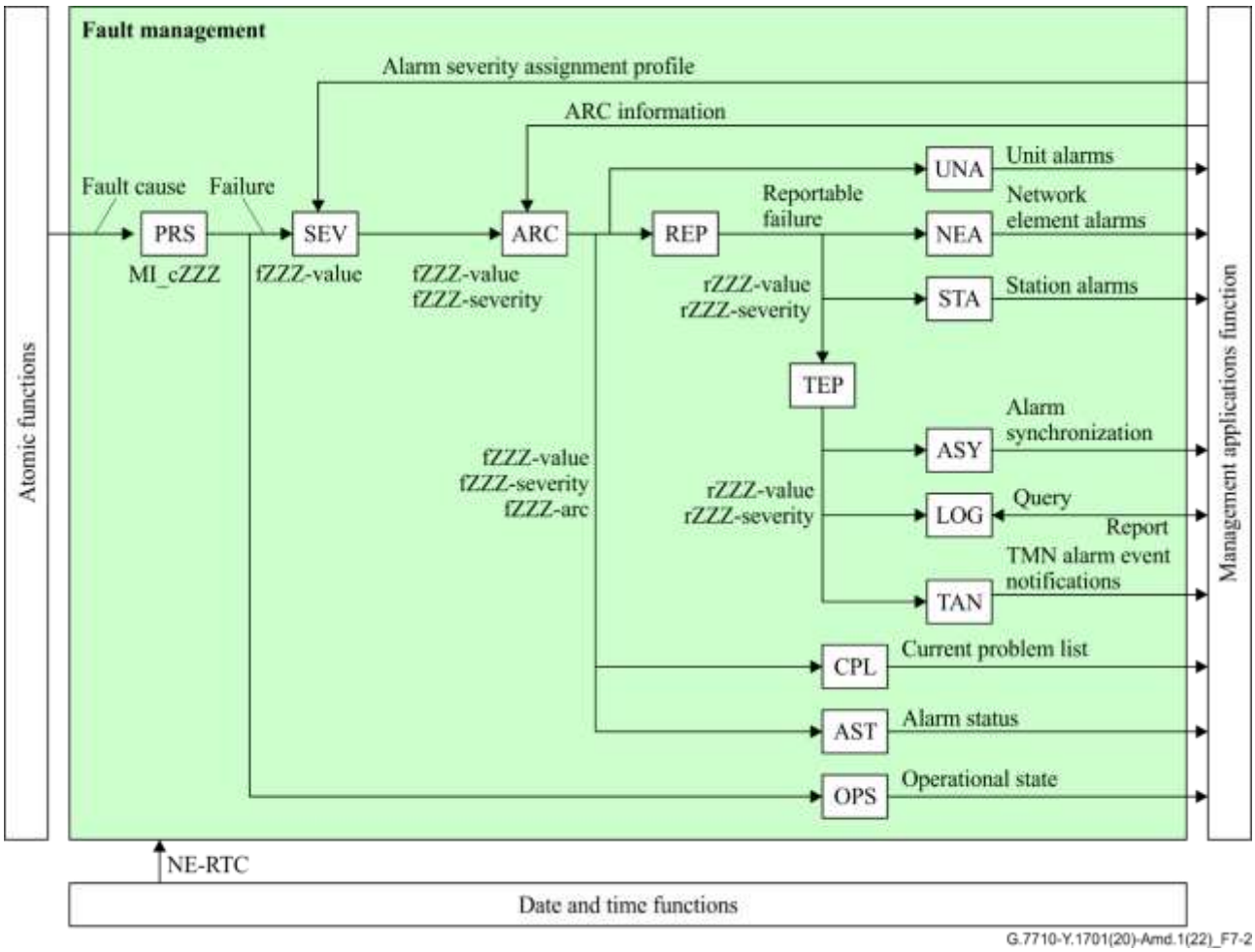


Figure 7-2 – Fault management inside the EMF

7.2.1 Fault cause persistency function – PRS

The EMF within the NE performs a persistency check on the fault causes before it declares that a fault cause is a failure.

The defect correlations provide a data reduction mechanism for the information on fault and performance monitoring primitives presented at the MP reference points.

The fault cause persistency function will provide a persistency check on the fault causes (that are reported across the MP reference points) before it declares that a fault cause is a failure. In addition to the transmission failures, hardware failures with signal transfer interruption are also reported at the input of the fault cause function for further processing. See Figure ~~8~~7-3.

Symbol:

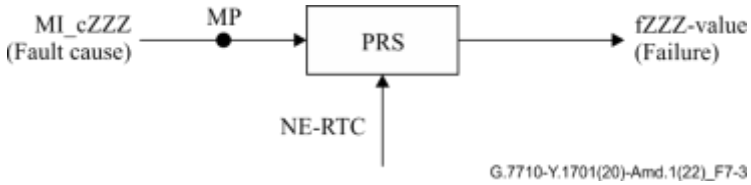


Figure ~~8~~7-3 – Fault cause persistency function

Interfaces:

Table 7-3 – Fault cause persistency input and output signals

Input(s)	Output(s)
MI_cZZZ NE-RTC	fZZZ-value

Processes:

The fault cause persistency function is responsible for the integration of fault causes MI_cZZZ-value into failures fZZZ-value.

A transmission failure (fZZZ-value) 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.

The failure declaration and clearing shall be time-stamped. For declaration, the time-stamp shall indicate the time at which the fault cause is activated at the input of the PRS. For clearing, the time-stamp shall indicate the time at which the fault cause is deactivated at the input of the PRS.

The fZZZ-value includes the identification of the managed entity and its location, an indication whether the failure has been raised or cleared, and a time-stamp of this event.

7.2.2 Severity assignment function – SEV

Symbol:

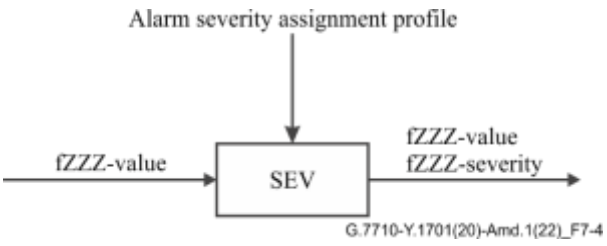


Figure ~~9~~7-4 – Severity assignment function

Interfaces:

Table 7-4 – Severity assignment input and output signals

Input(s)	Output(s)
fZZZ-value Alarm severity assignment profile	fZZZ-value fZZZ-severity

Processes:

The severity assignment function is responsible for assigning a value to the fZZZ-severity variable.

The assignment shall be possible per managed entity and is based on the alarm severity assignment profile.

The severity shall be expressed according to the specification in [ITU-T M.3100]:

- Critical, major, minor, warning, not alarmed.

The failure fZZZ-value accompanied with the assigned severity fZZZ-severity shall become available at the output.

7.2.3 Alarm reporting control function – ARC

The ARC function allows a management system to control the alarm reporting on a per-managed entity basis as defined in [ITU-T M.3100].

The ARC states that may be specified for a managed entity are defined in clause 7.1.3.2:

– the ALM state is required for all managed entities that can detect alarms;

– in addition, at least one of the states: NALM, NALM-TI or NALM-QI must be supported;

– if NALM-QI is supported, then NALM-NR is required, and NALM-CD is optional.

When an entity is put in the ARC state of NALM-QI, alarm reporting for the entity is turned off until the managed entity is free of all the failures specified in the ARC list.

Symbol:

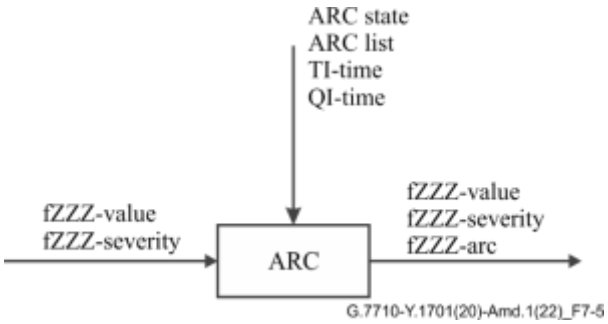


Figure ~~10~~7-5 – Alarm reporting control

Interfaces:

Table 7-5 – ARC input and output signals

Input(s)	Output(s)
fZZZ-value fZZZ-severity ARC state ARC list TI-time QI-time	fZZZ-value fZZZ-severity fZZZ-arc

Processes:

The ARC function is responsible for assigning a value to the fZZZ-arc variable.

The assignment shall be possible per managed entity and is based on the ARC information.

The fZZZ-arc value shall be "reported" when the ARC information specifies the probable cause to be "reported".

The fZZZ-arc value shall be "not reported" when the ARC information specifies the probable cause to be "not reported".

The failure value and severity accompanied with the assigned alarm status fZZZ-arc shall become available at the output.

Note that ARC information includes the ARC state (whether or not the managed entity is ARCing any failures) and the list of problems that has been requested to be suppressed. If the ARC state is in any state but ALM, the list of problems to be suppressed needs to be evaluated to determine whether or not the failure can be reported.

The ARC shall be implemented according to the specification in [ITU-T M.3100].

7.2.4 Reportable failure function – REP

Symbol:

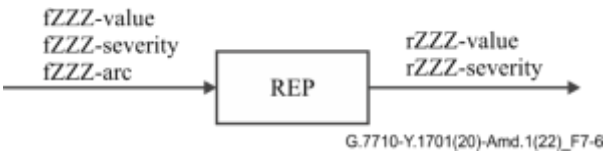


Figure ~~11~~7-6 – Reportable failure function

Interfaces:

Table 7-6 – Reportable failure input and output signals

Input(s)	Output(s)
fZZZ-value fZZZ-severity fZZZ-arc	rZZZ-value rZZZ-severity

Processes:

The reportable failure function is a filter, responsible for forwarding only those probable causes that have been identified as reportable alarms.

If the failure is not being controlled by ARC, or has an alarm severity assignment of "Not alarmed", the failure's value and severity shall become available at the output as rZZZ-value and rZZZ-severity. Otherwise, neither rZZZ-value nor rZZZ-severity shall become available at the output.

7.2.5 Unit alarms function – UNA

Symbol:

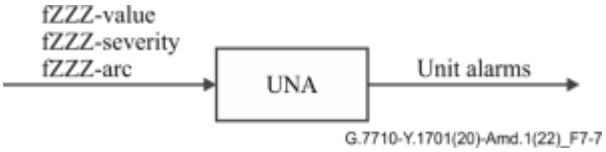


Figure ~~1~~7-7 – Unit alarms function

Interfaces:

Table 7-7 – Unit alarms input and output signals

Input(s)	Output(s)
fZZZ-value fZZZ-severity fZZZ-arc	Unit alarms

Processes:

The unit alarms function is responsible for determining whether or not unit audible/visual indicators need to be updated.

Effect of the alarm status upon audible/visual indicators is left undefined in this Recommendation. It is only illustrated here to show that alarm information is forwarded to this function for application-specific processing.

7.2.6 Network element alarms function – NEA

Symbol:

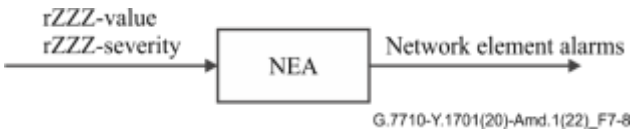


Figure ~~1~~7-8 – Network element alarms function

Interfaces:

Table 7-8 – Network element alarms input and output signals

Input(s)	Output(s)
rZZZ-value rZZZ-severity	Network element alarms

Processes:

The network element alarms function is responsible for determining whether or not aggregate audible/visual indicators need to be updated.

7.2.7 Station alarms function – STA

Symbol:

Figure ~~14~~7-9 – Station alarms function

Interfaces:

Table 7-9 – Station alarms input and output signals

Input(s)	Output(s)
rZZZ-value rZZZ-severity	Station alarms

Processes:

The station alarms function is responsible for determining whether or not aggregate station audible/visual indicators need to be updated.

7.2.8 TMN event pre-processing function – TEP

Symbol:

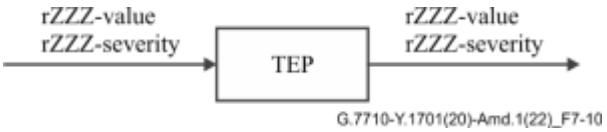


Figure ~~15~~7-10 – TMN event pre-processing function

Interfaces:

Table 7-10 – TMN event pre-processing input and output signals

Input(s)	Output(s)
rZZZ-value rZZZ-severity	rZZZ-value rZZZ-severity

Processes:

The TMN event pre-processing function (see [ITU-T X.734]) adds information such as correlated notifications. Generally, it adds information that is not determined or possible to determine by the object, but across multiple objects.

7.2.9 Alarm synchronization function – ASY

Symbol:

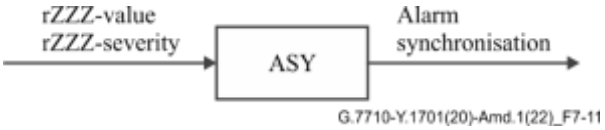


Figure ~~16~~7-11 – Alarm synchronization function

Interfaces:

Table 7-11 – Alarm synchronization input and output signals

Input(s)	Output(s)
rZZZ-value rZZZ-severity	Alarm Synchronization

Processes:

The alarm synchronization function is responsible for storing all current reportable alarm information. Storing means to support functions such as enhanced event control (see [ITU-T Q.821]).

7.2.10 Logging function – LOG

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. See [b-ITU-T X.735] for additional details.

Symbol:

Figure ~~1~~7-12 – Logging function

Interfaces:

Table 7-12 – Logging input and output signals

Input(s)	Output(s)
rZZZ-value rZZZ-severity Query	Report

Processes:

The log function provides a filter according to the "discriminator construct" defined in [ITU-T X.735]. The alarm records shall be stored. Upon query, the stored alarm information shall be reported.

7.2.11 TMN alarm event notifications function – TAN

Symbol:

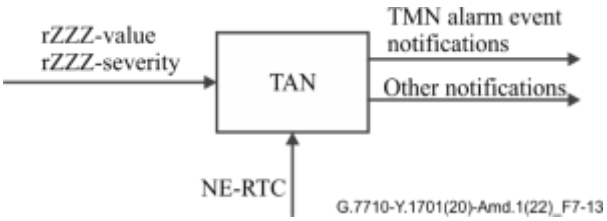


Figure ~~18~~7-13 – TMN alarm event notifications function

Interfaces:

Table 7-13 – TMN alarm event notifications input and output signals

Input(s)	Output(s)
rZZZ-value rZZZ-severity NE-RTC	TMN alarm event notifications Other notifications

Processes:

The TMN alarm event notifications function is responsible for filtering and forwarding event notifications (see "event forwarding discriminator" in [ITU-T X.734] and [ITU-T X.754]).

The TAN function uses the NE-RTC when time-stamping the time of the event report.

7.2.12 Current problem list function – CPL

Symbol:

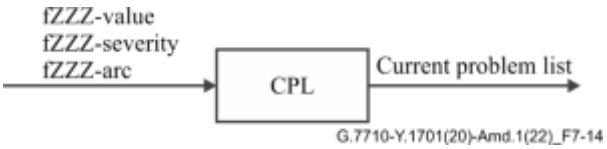


Figure ~~19~~7-14 – Current problem list function

Interfaces:

Table 7-14 – Current problem list input and output signals

Input(s)	Output(s)
fZZZ-value fZZZ-severity fZZZ-arc	Current problem list

Processes:

The current problem list function is responsible for updating the current problem list in each managed entity. The current problem list shall contain the failure and alarm status of all current declared failures regardless of whether they will not be sent as a notification.

7.2.13 Alarm status function – AST

Symbol:

Figure ~~20~~7-15 – Alarm status function

Interfaces:

Table 7-15 – Alarm status input and output signals

Input(s)	Output(s)
fZZZ-value fZZZ-severity fZZZ-arc	Alarm status

Processes:

The alarm status function is responsible for updating the alarm status of each managed entity. The alarm status indicates the occurrence of an abnormal condition relating to a managed entity. It may also function as a summary indicator of alarm conditions associated with a specific resource. It is used to indicate the existence of an alarm condition, a pending alarm condition such as threshold situations, or (when used as a summary indicator) the highest severity of active alarm conditions. When used as a summary indicator, the order of severity (from highest to lowest) is critical, major, minor, warning, not alarmed (refer to Table 7-2).

7.2.14 Operational state function – OPS

Symbol:

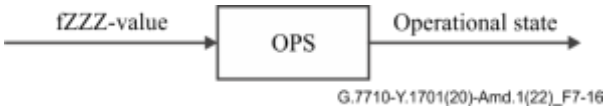


Figure ~~21~~7-16 – Operational state function

Interfaces:

Table 7-16 – Operational state input and output signals

Input(s)	Output(s)
fZZZ-value	Operational state

Processes:

The operational state function is responsible for updating the operational state in each managed entity, and optionally feeding into the operational state function for dependent managed entities.

The operational state defines whether the managed entity is able to partially, or fully, perform the service (enabled), or is totally inoperable (disabled). This is according to [ITU-T X.731].

8 Configuration management

Configuration management provides functions to exercise control over, identify, collect data from and provide data to NEs. Configuration management supports network planning and engineering, installation, service planning and negotiation, provisioning, and status and control.

Figure ~~22~~8-1 outlines the configuration management functions inside the EMF. In general, all these functions accept provisioning data from the MAF, perform a data check and return the check status to the MAF. Depending on the check status, it is decided to update the MIB related to the new provisioning data.

Some functions accept control information from the MAF, are able to provide reporting data to the MAF, and have access to the atomic functions by means of MI signals.

It is assumed that the configuration management functions alarm severity, report options, and PM thresholds only perform a data check. Subsequent processing is done in fault management and performance monitoring.

Furthermore, Figure ~~22~~8-1 is not intended to be a coherent functional model. It just lists the configuration management functions, and the interfaces with the atomic functions, the message communication function and the date and time function.

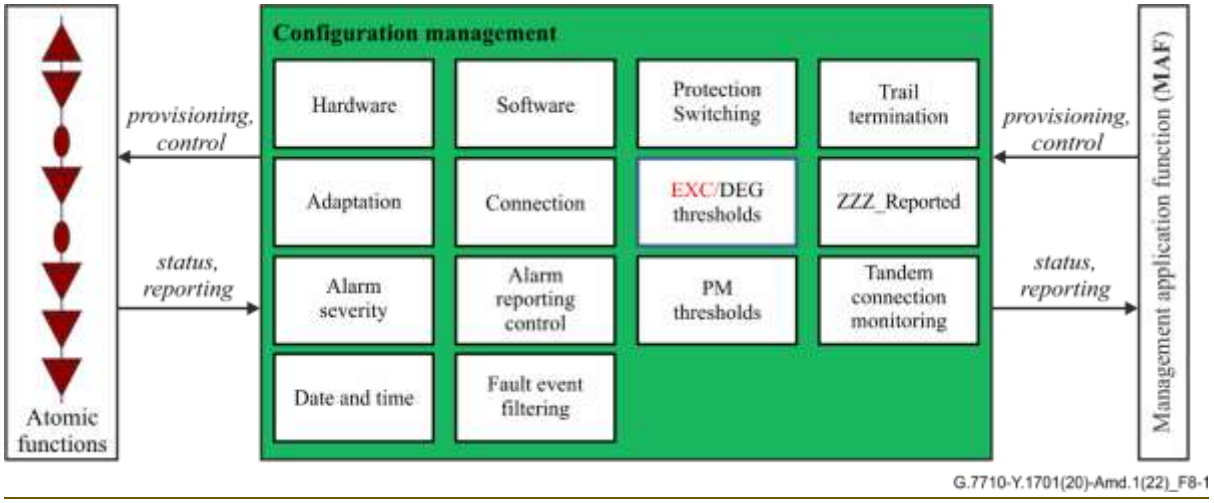


Figure ~~22~~8-1 – Configuration management inside the EMF

Within the scope of this Recommendation, i.e., the equipment management functions inside the NE, the applications are limited to provisioning and control and status reporting. The applications descriptions include the provisioning of the NE's hardware and software. It includes the provisioning of atomic functions by means of MI signals (as specified by the technology-specific Recommendations). It includes the provisioning of some of the FCAPS functions, like performance monitoring thresholds and protection switching schemes. This Recommendation does not include the MIB-related applications (e.g., upload and download).

8.1 Hardware

8.1.1 Provisioning

An NE should provide various functions that allow provisioning of the hardware such as slot provisioning, circuit pack assignment and port provisioning.

8.1.2 Inventory reporting

An inventory of the provisioned, or present hardware, must be reported on request of an external command.

8.2 Software

8.2.1 Provisioning

An NE may accept new software versions to be downloaded. The loading includes initialization and testing that the load is successful and back-out of the software if the load is not successfully completed. The NE will support in-service software upgrades, at minimum, between two consecutive versions of a software release. Note that during software switchover, some management services may be impacted. For example, creation of new services during this period may not be allowed.

In support of software download, NEs shall additionally support the software management requirements specified in clause 6 of [ITU-T X.744].

8.2.2 Inventory reporting

An inventory of the present software release is reported on request of an external command.

8.3 Protection switching

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

– operate/release manual protection switching
– operate/release force protection switching
– operate/release lockout
– request/set automatic protection switching (APS) parameters.

8.3.1 Provisioning

NEs may support one or more types of protection schemes:

– Trail protection (e.g., linear OMSP, linear MSP, MS SPring, VC)
– Subnetwork connection protection (e.g., VC, OCH, linear ETH).

Each scheme can be characterized by the set (or a subset) of the following parameters:

– topology (linear (see [ITU-T G.808.1]), ring (see ITU-T draft Rec. G.808.2)
– protection architecture (1+1, 1:n)
– switching type (unidirectional/single ended, bidirectional/dual ended)

– operation type (non-revertive, revertive)
– automatic protection switching (APS) channel (provisioning, usage, coding)
– protection switch requests
– protection switch performance
– protection switch state machine.

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

8.3.2 Reporting

The protection switching block in Figure ~~22~~8-1 reports the current status of protection switching (e.g., status of protocol state machine, condition of blocking port, etc.). Note that this reporting information is used to monitor the protocol status from outside the NEs. To realize this reporting, an atomic function shall report protocol-related state information to the EMF by means of MI signals (as defined in technology-specific recommendations). The protection switching state handling function is responsible for receiving and forwarding protocol-related state information to the MAF.

8.3.2.1 Protection switching (PS) state handling function

Symbol:

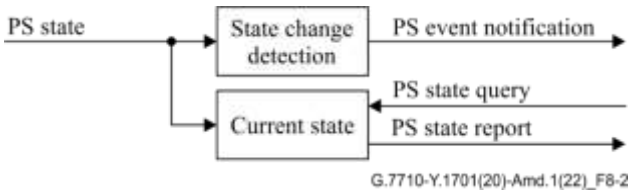


Figure ~~23~~ 8-2 – PS state handling function

Interfaces:

Table ~~17~~8-1 – PS state handing input and output signals

Input(s)	Output(s)
PS State (via MI signals) PS State Query	PS Event Notification PS State Report

Processes:

The PS state handling function is responsible for receiving and forwarding protocol-related state information to the MAF. The state change detection process detects a change of protocol state and autonomously notifies it as an event signal (PS Event Notification) when an input signal (PS State) changes. The current state process latches the latest protocol state and reports the information (PS State Report) when the MAF requests it on-demand basis (via PS Event Query).

8.4 Trail termination

The purpose of the trail termination is to generate, add and monitor information concerning the integrity and supervision of adapted information. This includes:

– connectivity supervision
– continuity supervision
– signal quality supervision
– processing of maintenance information (forward/backward indications).

8.4.1 Provisioning

8.4.1.1 Trail trace identifier

The TTI is used to ensure proper connection between network elements and to generate a trail trace identifier mismatch alarm if the accepted value is different from the expected value. The TTI is useful in meshed network topology with cross-connects that have several input and output ports. TTIs are also a means for the OS to deduce the network topology. Specifically, the OS gets the list of source and sink TTIs of all network elements and can automatically deduce the trails at a specific layer by a comparison of the expected TTIs of the sink objects and the TTIs sent from the source objects.

The trail trace identifier (TTI) process needs to be provisioned with the TTI to transmit, with the expected TTI, and with a qualifier to determine the trace identifier mismatch detection. The provisioning can be under control of the management plane, the control plane, or a combination of both.

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

– provisioning of source TTI
– provisioning of the expected TTI
– enable/disable detection of trace identifier mismatch (TIM)
– enable/disable TIM consequent action.

The source TTI and the expected TTI are communicated to the trail termination functions from the EMF via management signals at the management points.

The detection mode for TIM is communicated to an atomic function from the EMF via the management signals at the management points.

An atomic function shall report, at the request of the EMF, the value of the received and accepted TTI via the management signals at the management points. The TIM consequent action enabling/disabling control signal is communicated to an atomic function from the EMF via management signals at the management points.

8.4.1.2 Maintenance entity group identifiers

For packet transport networks, three types of maintenance entity identifiers are defined for connectivity checking:

– MEGID "maintenance entity group (MEG) identifier"
– MEPID "MEG end point identifier"
– MIPID "MEG intermediate point identifier".

These identifiers are used to ensure proper connectivity between the endpoints of a maintenance entity group and to generate a:

– mismerge;
– loss of continuity; or
– unexpected MEP.

alarm if the received value is different from the expected value. The identifiers are useful in meshed network topology with matrix connection and FDFrs that have several input and output ports to check continuity and connectivity between all ports.

The connectivity check process needs to be provisioned with the identifiers to transmit, with the expected identifiers, and enable/disable the connectivity check process. The provisioning can be under the control of the management plane, the control plane, or a combination of both.

The functions that allow a user to provision the operation of a connectivity check process are:

– provisioning of the MEGID and the local MEPID

– provisioning of the remote MEPIDs

– enable/disable connectivity checking.

The identifiers are communicated to the trail/flow termination functions from the EMF via management signals at the management points.

An atomic function shall report, at the request of the EMF, the content of the connectivity check fields via the management signals at the management points.

8.4.2 Reporting

8.4.2.1 Trail trace identifier

The TTI process supports the reporting of the accepted TTI.

8.4.2.2 Maintenance identifiers

The connectivity check process supports the reporting of the received connectivity check frame/packet.

8.5 Adaptation

8.5.1 Provisioning

Access points which have multiple adaptation functions connected to them, allowing different client signals to be transported via the server signal, need a selection of the active client. The selection of the active client can be provisioned by means of the activation of the related adaptation function. For cases where an access point has a single adaptation function connected, and supports a single client signal only, the selection is fixed. Table ~~18~~8-2 gives an overview of the provisioning items and the MI signals, including range and defaults, used to configure the appropriate atomic functions.

Table ~~18~~8-2 – Payload structures provisioning

Provisioning	Management information (MI)		
	MI signal	**Value range**	**Default**
– activation of adaptation function	MI_Active	true, false	false

8.5.2 Reporting

An atomic function will report on request the value of the received and accepted payload type signal. See clause 7.1.1.1, payload type supervision, for details. Table ~~19~~8-3 gives an overview of the reporting items and the MI signals, including range and defaults, received from the appropriate atomic functions.

Table ~~19~~8-3 – Payload structures reporting

Reporting	Management information (MI)		
	MI signal	**Value range**	**Default**
– received and accepted path signal label	MI_AcSL	application-dependent	N/A

8.6 Connection

8.6.1 Provisioning

A connection function is surrounded by connection points (CPs)/flow points (FPs) and termination connection points (TCPs)/termination flow points (TFPs). Each TCP/TFP is identified via the API associated with its trail termination function, and each CP/FP is identified via the API associated with its adaptation function, extended with a (if applicable) tributary signal number (see Figures ~~24~~8-3, ~~25~~ 8-4 and ~~26~~8-5).

Reconfigurable network elements provide connection capabilities at specific layers. Cross-connections can be configured between all attached ports.

The following provisioning functions are identified:

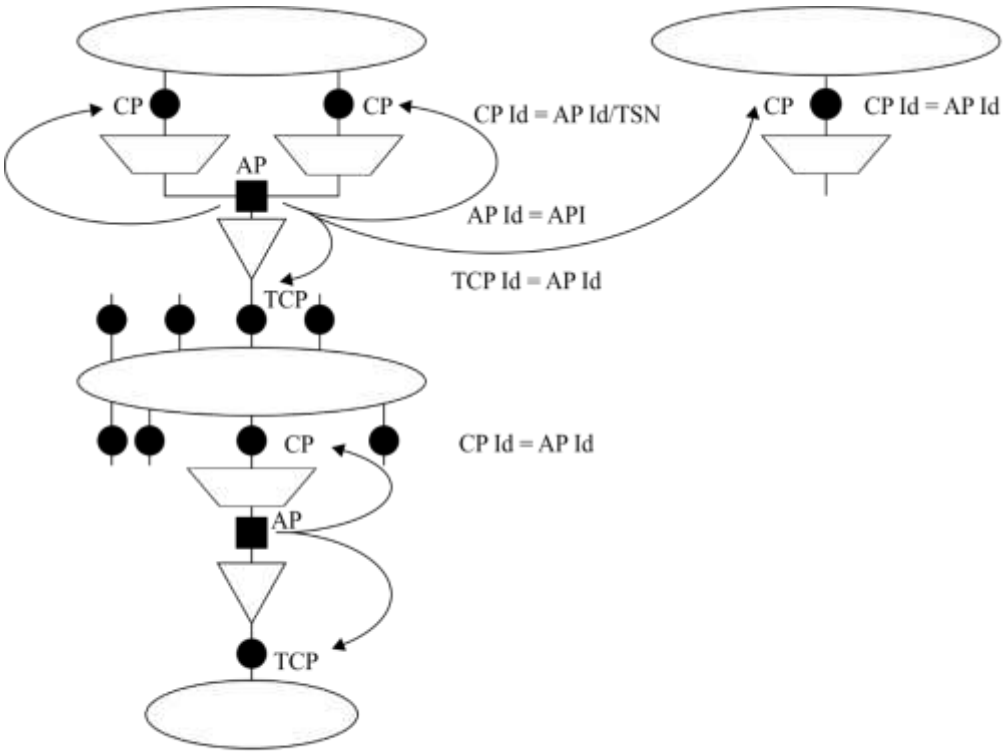
1) Create a
   - point-to-point (unidirectional or bidirectional)
   - point-to-multipoint (unidirectional)
   - multipoint-to-multipoint (bidirectional)
   - rooted multipoint (bidirectional)
   - matrix connection and FDFr.
2) Remove a
   - point-to-point (unidirectional or bidirectional)
   - point-to-multipoint (unidirectional)
   - multipoint-to-multipoint (bidirectional)
   - rooted multipoint (bidirectional)
   - matrix connection or FDFr.

For the case of a trail protection, the access points (APs) 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 CPIds when the interface changes from unprotected to protected and vice versa.

A matrix connection is therefore characterized by a set of CP/FP or TCP/TFP identifiers connected to each other. Table ~~20~~8-4 gives an overview of the provisioning items and the MI signals, including range and defaults, used to configure the appropriate atomic functions.

Table ~~20~~8-4 – Matrix connections provisioning

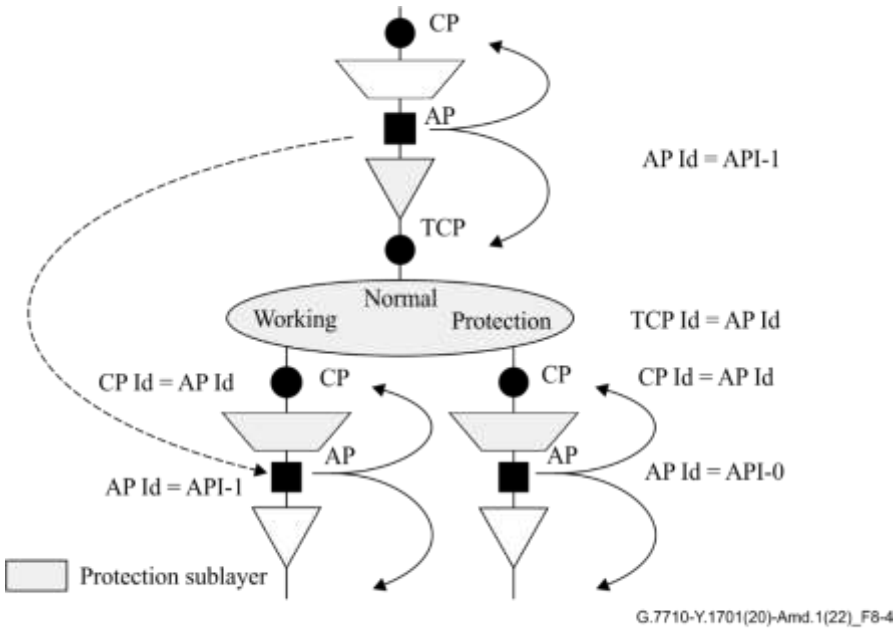
Provisioning	Management information (MI)		
	MI signal	**Value range**	**Default**
– matrix connection	MI_ConnectionPortIds	set of (T)CP/FP Ids	no default
	MI_ConnectionType	unprotected, 1+1 protected, …	no default
	MI_Directionality	unidirectional, bidirectional	no default



NOTE – While this figure is drawn in the context of circuit-based terminology, the same figure is valid for packet-based terminology by replacing CP by FP and TCP by TFP.

G.7710-Y.1701(20)-Amd.1(22)_F8-3

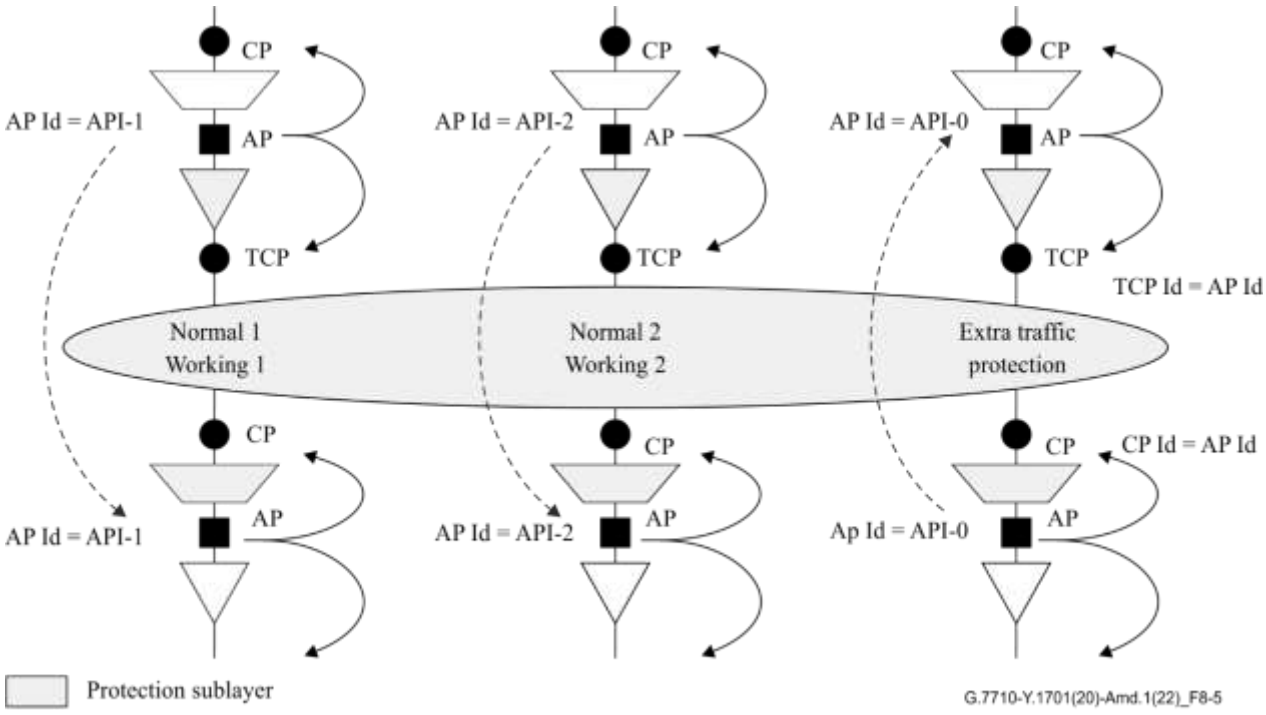
Figure ~~24~~ 8-3 – CP/FP and TCP/TFP identification scheme



G.7710-Y.1701(20)-Amd.1(22)_F8-4

NOTE – While this figure is drawn in the context of circuit-based terminology the same figure is valid for packet-based terminology by replacing CP by FP and TCP by TFP.

Figure ~~25~~ 8-4 – CP/FP and TCP/TFP identification scheme for the case of 1+1 trail protection



NOTE – While this figure is drawn in the context of circuit-based terminology the same figure is valid for packet-based terminology by replacing CP by FP and TCP by TFP.

Figure ~~26~~ 8-5 – CP/FP and TCP/TFP identification scheme for the case of 1:n trail protection

8.6.2 Reporting

The following reporting functions are identified:

1) *Get connectivity capabilities*:

   Because reconfigurable network elements may have static cross-connection restrictions, the OS should be aware of these restrictions.

   This function gives an overview of the fabric's static capability to connect termination points. This is done by identifying one or more sets of termination points which can be interconnected.

   Restrictions of connectivity may be caused by principal design of the switch matrix or by the fact that not all sink termination points are fully reachable from all source termination points.

   This function should not take limited processing capacity, usage, or current problems into account. These additional restrictions have to be considered dynamically by the OS.

2) *Report connectivity changes of a cross-connect*:

   The NE has to send a report when the connectivity of the fabric changes. Note that after receiving a report about connectivity changes, the OS may again get all connectivity sets to update its connectivity topology.

3) Report the creation of a point-to-point cross-connection.

4) Report the deletion of a point-to-point cross-connection.

5) Report the suspend/resume of traffic on a point-to-point cross-connection.

6) *Get all point-to-point cross-connections*:

   This action returns the list of all point-to-point cross-connections created.

8.7 Threshold of error distribution defects ~~EXE and DEG thresholds~~

The EXE and DEG threshold MI signals are sent to the AF from the EMF to set thresholds of the EXE and DEG defects. Defect of excessive error (EXE) or degraded signal (DEG) depend on the distribution of errors in the network. Excessive error defect (dEXE) and degraded signal defect (dDEG) could be supported by Poisson mode distribution and only degraded signal defect (dDEG) could be supported by burst distribution. The application of Forward Error Correction (FEC) and Decision Feedback Equalizer (DFE) will make the error distribution as burst mode. The applicability of each mode to specific technology is specified in technology specific recommendations such as [ITU-T G.874], [ITU-T G.8052], etc.

8.7.1 Provisioning

The threshold and monitor period of the burst-based degraded defect process requires provisioning. Table ~~2~~18-5 gives an overview of the provisioning items and the MI signals, including range and defaults, used to configure the appropriate atomic functions.

Table ~~2~~18-5 – Error defect threshold provisioning ~~DEG threshold provisioning~~

Provisioning	Management information (MI)		
	MI signal	Value range	Default
– Poisson-based excessive defect threshold	MI_EXC_X	10^{-3},10^{-4}, 10^{-5}	10^{-3}
– Poisson-based degraded defect threshold	MI_DEG_X	10^{-5}, 10^{-6}, 10^{-7}, 10^{-8}, 10^{-9}	10^{-6}
– Burst-based degraded defect interval threshold	MI_DEGTHR	0..N EBs or 0..100%	SES estimator
– Burst-based degraded defect monitor period	MI_DEGM	2..10	7

The provisioning of these signals is individual per trail in the NE.

8.8 Defect reporting control ~~ZZZ_Reported~~

8.8.1 Provisioning

The reporting of certain "secondary defects" is optional. Secondary defects are the result of a consequent action on a "primary defect" in another network element. The ZZZ_reported MI signal sent to the AF from the EMF is used to control the defect reporting, and is defined in the technology-specific Recommendations. The control of the reporting is by the parameter MI_ZZZ_Reported defined in the technology-specific Recommendations.

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.

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

8.9 Alarm severity assignment

8.9.1 Provisioning

The severity assignment function (SEV, see clause 7.2.2) inside fault management requires the provisioning of an alarm severity assignment for the managed entities. Table ~~22~~8-6 gives an overview of the provisioning items, including range and defaults. Note that the provisioning is not related to an atomic function.

Table ~~22~~8-6 – Alarm severity provisioning

Provisioning	Value range	Default
– alarm severity assignment per managed entity	Critical, major, minor, warning, not alarmed	For primary failures: (event and equipment-specific)
		For secondary failures: Not Alarmed

8.10 Alarm reporting control (ARC)

8.10.1 Provisioning

The ARC function (see clause 7.2.3) inside fault management requires the provisioning of the ARC mode per instance. Table ~~23~~8-7 gives an overview of the provisioning items, including range and defaults. Note that the provisioning is not related to an atomic function.

Table ~~23~~8-7 – ARC provisioning

Provisioning	Value range	Default
– ARC state	ALM, NALM, NALM-TI, NALM-QI	Technology-specific
– ARC list of probable causes to suppress	Application-dependent	N/A
– TI-time	0..99 hours with 1-minute granularity	see [ITU-T M.3100]
– CD-time	0..99 hours with 1-minute granularity	see [ITU-T M.3100]

8.11 PM thresholds

Most services are offered to customers with a predefined level of availability (e.g., standard service, premium service, etc.). For each service, a set of PM threshold values will be defined to supervise the fulfilment of the availability. This set of PM thresholds is common for all termination points that carry traffic of the same service. Changes in the quality of the service offered to the customer lead to a change in the associated threshold value set in every termination point carrying this kind of service.

Therefore, PM thresholds are set by assigning a threshold value profile to the termination points to be supervised. This functionality provides the ability to change PM thresholds for a group of termination points at the same time by changing only the values in the assigned profile. Default profiles which are assigned to every newly created termination point are configurable during creation time.

8.12 Tandem connection monitoring (TCM) activation

8.12.1 Provisioning

If a TCM function needs to be activated at a CTP, which already has activated TCM functions, the traffic may not be affected. Figure ~~27~~8-6 outlines the possibilities. The upper part shows the initial situation at the CTP with TCM functions A and B activated. When the operator has to provision a new TCM, he/she must know the required position of the new TCM in relation to the existing TCMs A and B. In general, three insertion points are possible:

1) left to the most left;

2) between two others; and

3) right to the most right.

This is illustrated in the lower part of Figure ~~27~~8-6.

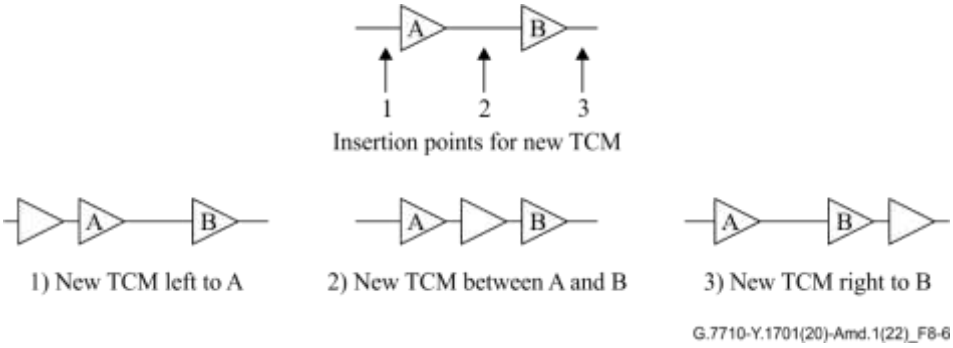


Figure ~~27~~8-6 – TCM activation provisioning

From the NE point of view, two behaviours are possible.

– The NE provides flexible allocation of new TCM functions. In this case, the operator only has to specify the location of the new TCM function, in relation to the existing ones, at the same CTP.

– The NE provides no flexibility. The order of the TCM functions at the CTP is fixed. In this case, the operator may have to rearrange existing functions in order to free the location for the new function. This rearrangement should be hitless for the traffic. However, inconsistencies in the supervision process might not be avoided.

8.13 Date and time

The date and time functions comprise the local real-time clock (RTC) function and the performance monitoring clock (PMC) function. The message communication function (MCF) is able to set the local real-time clock function. The date and time is incremented by the local real-time clock function. The FCAPS functions that need date and time information, e.g., to time stamp event reports, get this information from the date and time functions.

The requirements for the local real-time clock function and the performance monitoring clock are specified in clause 8.13.2. These requirements are based on the date and time applications, described in clause 8.13.1.

The following abbreviations are used for the times in this clause:

C The adjustment in time to compensate for delivery delay.

S The difference in time between the arrival of the time signal at the edge of the NE and the time indicated on the local real-time clock, immediately after a reset local clock request has been completed.

X The delivery delay of the time signal from the external time reference to the edge of the NE.

Y The drift of the local real time clock within a 24-hour interval of the external time reference.

Z The difference between the time that a prescribed event is detected by the NE and the time that the NE assigns to this event.

8.13.1 Date and time applications

The three identified applications related to date and time are the capabilities to time-stamp event reports (e.g., alarms), to monitor clock signals and to schedule activities.

8.13.1.1 Time-stamping

A number of functions/processes and reports require a relatively precise and consistent current time. The NE local real-time clock function provides this time information. [ITU-T M.2140] suggests that faults and performance degradations should be correlated to the root cause problem. To meet this need, time-stamping of the event data is essential, see Figure ~~28~~8-7.

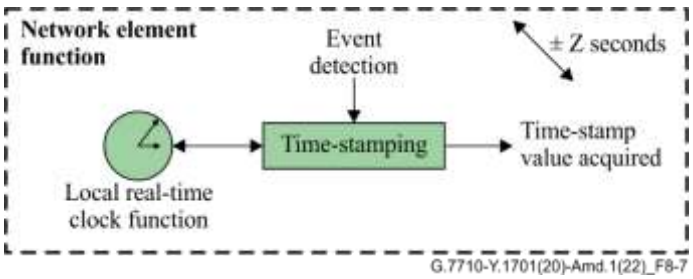


Figure ~~28~~8-7 – Illustration of time-stamping

Events, performance reports and registers, containing event counts or gauge values that require time-stamping shall be time-stamped with a resolution of one second relative to the NE local real-time clock function. This resolution exceeds some of the specifications in [ITU-T M.2120]. The date/time-stamps shall be according to the coordinated universal time (UTC), containing day, month, year, hour, minute and second. The display of this date/time-stamps may be done in local time by applying the appropriate offset to the UTC time.

Events and reports shall be time-stamped as follows:

1) The time-stamp for fault events (declaration/clearing) shall indicate the start of the fault cause prior to failure integration time.

2) The performance measurement intervals shall contain the time-stamp associated with the measurement interval. This is, for example, consistent with the periodEndTime attribute in the historyData object class defined in [ITU-T Q.822].

3) The time-stamp for threshold report (TR) declaration and reset threshold report (RTR) declaration shall indicate the time of the event according to the performance monitoring clock (see clause 8.13.1.2). This is consistent with [ITU-T M.2120].

4) All other requests and reports shall contain the time-stamp associated with the actuation.

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

The symbol Z in Figure ~~28~~ 8-7 represents the difference between the time that a prescribed event is detected by the NE and the time that the NE assigns to this event. It is an objective that the value of Z is less than, or equal to, one second. Specifications of Z are defined in the technology-specific ITU-T Recommendations.

8.13.1.2 Performance monitoring clock signals

Performance monitoring functions ensure, among others, the summation of one second event counts during 15-minute and 24-hour intervals. The start of such an interval is equal to the end of the previous interval. There is a need to have a signal that indicates the start/end of a one second interval, a signal that indicates the start/end of a 15-minute interval and a signal that indicates the start/end of a 24-hour interval. The 15-minute intervals are aligned with the quarter of an hour, i.e., 00:00, 15:00, 30:00 and 45:00. The 24-hour interval starts by default at midnight (00:00:00) and no modification is recommended. In order to compare 24-hour intervals between network providers for connections, which span many time zones, it is necessary to have the ability to start the 24-hour intervals at midnight (00:00:00) UTC.

8.13.1.3 Activity scheduling

A feature of NEs is the capability to schedule activities in advance.

Examples of scheduled activities are performance monitoring reporting, integrity checking to be performed at regular intervals, and the provisioning of a cross-connection at a certain date and time.

Figure ~~29~~8-8 outlines the mechanism of activity scheduling.

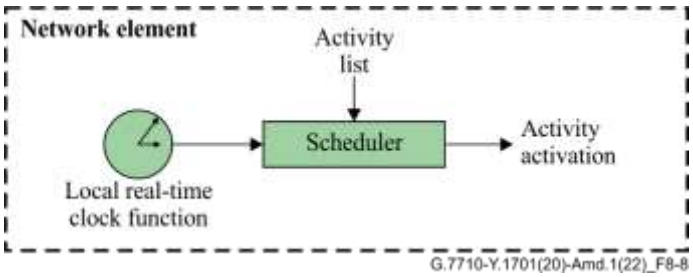


Figure ~~29~~ 8-8 – Activity scheduling

The activity list contains the activities along with their activation date and time. The latter may be indicated by a specific date and time (e.g., at 8.00 am Monday 15 October, 2007) or by a repetition (e.g., at 8.00 am Mondays).

The scheduler continuously compares the date and time of the local real-time clock function with the activation date and time indicators in the activity list. When there is a match, the related activity is activated.

8.13.2 Date and time functions

There are three date and time functions defined. The local real-time clock (RTC) function is required for time-stamping and activity scheduling. The capabilities to align the local real-time clock function to an external clock reference, which are essential to give proper support for the date and time applications. The performance monitoring clock (PMC) function, in addition to RTC, is typical for digital counter measurements.

8.13.2.1 Local real-time clock function

Symbol:

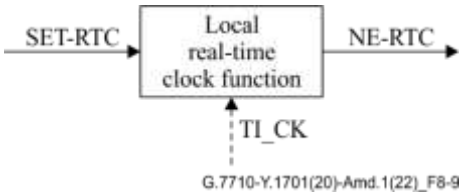


Figure ~~30~~8-9 – Local real-time clock function

Interfaces:

Table ~~24~~8-8 – Local real-time clock function input and output signals

Input(s)	Output(s)
SET-RTC TI_CK	NE-RTC

Processes:

The local real-time clock function is a logical entity within the NE providing date and time information to equipment management functions within the NE. The following requirements apply:

1) The local real-time clock function may be a free running clock or may be locked to any available clock source (e.g., equipment clock TI_CK).
2) The local real-time clock function shall have a resolution of 100 ms.
3) On receipt of a SET-RTC request, the local real-time clock function shall be set to the date and time specified by the SET-RTC request.
4) When the SET-RTC request is received, the difference in time between the management request at the input of the NE and the resultant NE-RTC shall be within S-C seconds.
5) The stability of the local RTC function shall be such that within 24 hours after a setting, the deviation shall not be greater than ±Y seconds.
6) The events and reports shall be time-stamped. The time-stamp should not result in a Z second difference from the local real-time clock function.
7) When the SET-RTC request causes an NE-RTC correction in magnitude of a difference greater or equal to 10 s, the NE shall emit a data change notification (e.g., attribute value change notification).

8.13.2.2 Local real-time clock alignment function with external time reference

A feature of NEs is the capability to align the local real-time clock function with an external time source.

An example of a general external time reference source is the Greenwich Mean Time (GMT)-based clock. Such a clock signal can be distributed by a radio broadcast station (e.g., GPS) or through a data network (e.g., IP or CMISE).

Figure ~~31~~ 8-10 depicts the relationship between an NE's local real-time clock (RTC) function and an external time reference.

The symbol X represents the delivery delay of the time signal from the external time reference to the edge of the network element. For a radio frequency-based time distribution, the value of X will be approximately zero. For an IP-based time distribution, not only X but also the variation of X could

be several seconds. X accounts for time accuracy losses in the server time protocol function (e.g., signal encoding) and in the distribution network. The specifications for values of X are outside the scope of this Recommendation.

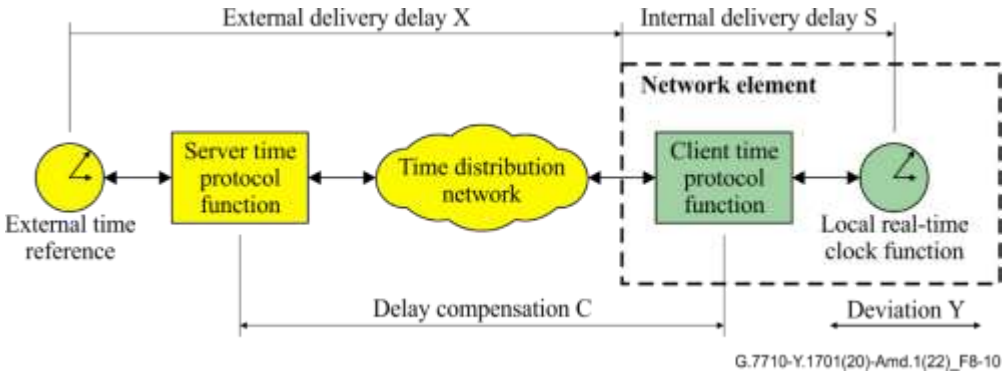


Figure ~~3~~18-10 – Local RTC function alignment with an external time reference

The symbol S represents the difference in time between the arrival of the time signal at the edge of the NE, and the time the corrective actions start on the local real-time clock function. S accounts for time accuracy losses introduced in the client time protocol function (e.g., signal acceptance and decoding). It is an objective that the value of S is less than or equal to 0.3 seconds. Specifications of S are defined in the technology-specific ITU-T Recommendations.

The symbol Y represents the drift of the local real-time clock function within a 24-hour interval of the external time reference, under the condition that no time resets have occurred during the 24-hour interval. It is an objective that the value of Y is such that S + Y + Z is less than or equal to 1.5 seconds. Specifications of Y are defined in the technology-specific ITU-T Recommendations.

The symbol C represents the adjustment in time to compensate for delivery delay. Various compensation protocols can be applied. A simple example is the compensation with a fixed value (C = constant) or no compensation at all (C = 0). The network time protocol, as specified in [b-IETF RFC 1305], is an advanced protocol able to compensate for the external and internal delivery delay (C = X + S). Appendix II outlines a mechanism of a relatively simple protocol to set the local real-time clock function within a few seconds relative to the external time reference. The specification of protocols and values of C are outside the scope of this Recommendation.

With the previous definitions, the difference in time between the local real-time clock function and the external time reference, within 24 hours after a reset local clock, shall not exceed X + S – C ± Y.

To compensate for the drift Y, the local real-time clock function is to be realigned with the external time reference on a regular basis. This realignment period should be determined so that the correction is less than 10 s to prevent all active performance monitoring functions (PMFs) from declaring suspect intervals.

8.13.2.3 Performance monitoring clock function

Symbol:

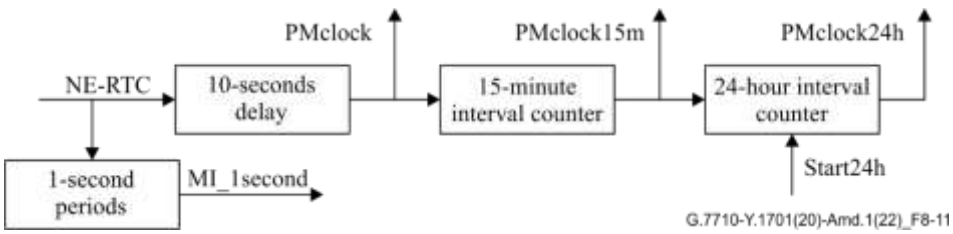


Figure ~~3~~2-8-11 – Performance monitoring clock function

Interfaces:

Table 258-9 – Performance monitoring clock input and output signals

Input(s)	Output(s)
NE-RTC Start24h	PMclock PMclock15m PMclock24h MI_1second

Processes:

The performance monitoring clock is a logical entity within the NE providing date and time information and clock signals to performance monitoring functions within the network element. The following requirements apply:

1) The **1-second periods** function shall generate the 1-second signal (MI_1second) at the end of each 1-second period as indicated by the NE-RTC.

2) The **10-second delay** function shall generate the date and time (PMclock), which is 10 s delayed with respect to the NE-RTC.

3) The **15-minute interval counter** shall generate 15-minute period indications (PMclock15m), which are aligned with the end of each quarter of an hour period (00:00, 15:00, 30:00, 45:00) with respect to PMclock. The start of a period is equal to the end of the previous period. If the NE-RTC is not reset, each 15-minute period spans 900 one-second periods.

4) The **24-hour interval counter** shall generate 24-hour period indications (PMclock24h), which are aligned with the end of a quarter of an hour period (00:00:00, 00:15:00, 00:30:00, …23:45:00) with respect to PMclock. The start of a period is equal to the end of the previous period. If the NE-RTC is not reset, each 24-hour period spans 86 400 one-second periods.

5) The **24-hour interval counter** may be instructed (by means of the Start24h signal) on when to begin the 24-hour period. The default period start time shall be 00:00 on the PMclock. By means of the Start24h signal, it shall be able to begin at the start of any 15-minute period.

It must be noted that the delay of 10 s is an example, based on the availability definition for SDH.

~~**8.14 Optical power monitoring and control**~~

~~This clause describes the management requirements for the optical power for the G.698.2 application in support of access link power monitoring and power control.~~

~~**8.14.1 Optical power monitoring**~~

~~For further study~~

~~**8.14.2 Optical power control**~~

~~For further study~~

8.145 Fault event filtering

8.145.1 Provisioning

The fault event filtering (FEF) function of the fault reporting management requires the provisioning of the FEF information (see clause12.1.2) to configure which received faults from the atomic function shall be reported out of the transport element. Table 268-10 gives an overview of the provisioning items, including value range and default. The FEF list is a list of faults, which are allowed to be

reported for triggering SDN controller-based restoration. Fault in the list should be within all the possible faults of the relevant atomic functions of the managed entity. Possible faults of atomic functions are defined in the transport technology-specific Recommendations.

Table ~~26~~8-10 – FEF provisioning

Provisioning	Value range	Default
FEF list per managed entity	Managed entity-dependent	Empty list

8.15 Administrative state

The Administrative State is defined in clause 8.1.1.3 of [ITU-T X.731], and consists of~~:~~ the following three values:

– LOCKED

– SHUTTING DOWN

– UNLOCKED

Events that trigger the transition between the state values of the Administrative state are defined in clause 7.1.3 of [ITU-T X.731]. Figure 8-12 is Figure 3 of [ITU-T X.731] illustrating the valid transition of the Administrative state.

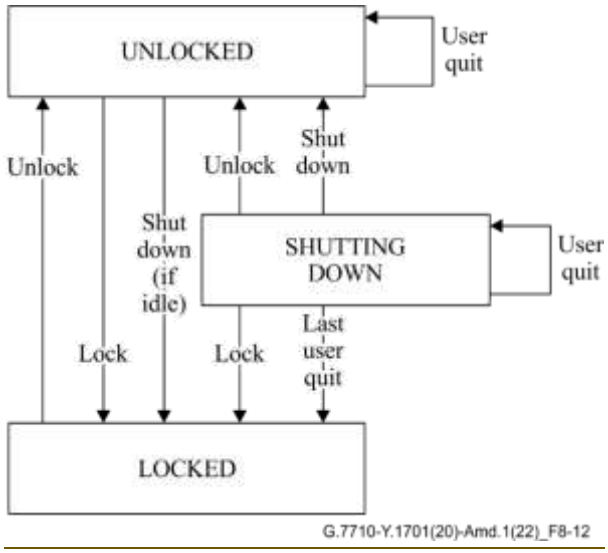


Figure 8-12 – Administrative state diagram (From Figure 3 of [ITU-T X.731])

Note that in the state transition diagram, the events "Unlock", "Lock" and "Shut down" could be initiated on the request of a management control system (MCS), such as SDN controller or EMS, etc.

Some resources exhibit only a subset of the possible administrative state values. Some resources cannot be locked, and hence exhibit only the *UNLOCKED* state. Other resources cannot be shut down gracefully, and hence do not exhibit the *SHUTTING DOWN* state. In general, the atomic functions in the transport equipment (such as those specified in [b-ITU-T G.798], [b-ITU-T G.8021] and [b-ITU-T G.8121.x] series) do not exhibit the SHUTTING DOWN state; and the LOCKED state is applicable only to some adaptation functions.

The actual subset of administrative state values supported varies from one type of resource to another and is specified in the technology-specific Recommendations.

Note that in some technology-specific Recommendations, the terms NORMAL or NOT_LOCKED have been used in place of the UNLOCKED state.

An operator can administratively lock a server layer trail in order to perform maintenance operations on the trail. When a server layer trail is locked, the user traffic on all its client layer connections is not allowed to be transmitted to nor received from that trail. In this situation, an alarm shall not be raised on the client layer connections due to the administrative blocking of user traffic. To lock a server layer trail, the locking instruction (i.e., administrative state is LOCKED) shall be applied to the adaptation function(s) at the end(s) of the server layer trail, as defined in clause 5.6.3 [ITU-T G.806]. Whether the EMF will send administrative lock instruction(s) to the adaptation function or individual client CPs, will be specified in the technology-specific equipment specification.

An operator can administratively lock a tandem connection in order to perform maintenance operations on the tandem connection. When a tandem connection is locked, the user traffic is not allowed to be transmitted on the tandem connection. In this situation, an alarm shall not be raised on the tandem connection due to the administrative blocking of the tandem connection. To lock a tandem connection, the locking instruction (i.e., administrative state is LOCKED) shall be applied to the adaptation function(s) at the end(s) of the tandem connection, as defined in clause 5.6.3 [ITU-T G.806].

Appendix IV provides examples for applying the administrative states on a server layer trail and tandem connection monitoring (TCM).

9 Account management

~~For further study.~~No transport specific account management specification is specified in this Recommendation.

10 Performance management

Performance management provides functions to evaluate and report upon the behaviour of telecommunication equipment and the effectiveness of the network, or NE. Its role is to gather and analyse statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network, NEs or other equipment, and to aid in planning, provisioning, maintenance and the measurement of quality. As such, it is carrying out the performance measurement phase of [ITU-T M.20].

The requirements for the performance monitoring functions are specified in clause 10.2. These requirements are based on the performance management applications, described in clause 10.1.

10.1 Performance management applications

The four basic performance management applications according to [ITU-T M.3400] are:

– *Performance quality assurance*

  Performance quality assurance supports decision processes that establish the quality measures that are appropriate to the area of performance management.

– *Performance monitoring*

  Acute fault conditions will be detected by alarm surveillance methods. Very low rate, or intermittent, error conditions in multiple equipment units may interact resulting in poor service quality and may not be detected by alarm surveillance. Performance monitoring is designed to measure the overall quality, using monitored parameters in order to detect such degradation. It may also be designed to detect characteristic patterns of impairment before signal quality has dropped below an acceptable level.

– *Performance management control*

  Performance management control supports the transfer of information to control the operation of the network in the area of performance management. For transport performance

monitoring, this application includes the setting of thresholds and data analysis algorithms and the collection of performance data, but has no direct effect on the managed network.

– *Performance analysis*

  Performance data may require additional processing and analysis in order to evaluate the performance level of the entity. The NE may be capable of carrying out part of the analysis of the data before a report is sent to the TMN.

Within the scope of this Recommendation, i.e., the equipment management functions inside the NE, the applications are limited to the collection and reporting of performance data. This performance data is gathered, pre-processed and partly analysed in the NE for the purpose of maintenance, bringing-into-service, quality of service, reporting and thresholding.

10.1.1 Concepts of "near-end" and "far-end"

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 presents 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, presents the performance of the two directions of the trail.

For maintenance or performance purposes, not only the measurements themselves are of importance, but also the locations where these measurements are done. Single-ended maintenance (SEM) is the ability to supervise both directions of the signal transmission from a single end of the connection. This is of particular importance if one end of the connection is terminated in an "unmanaged NE".

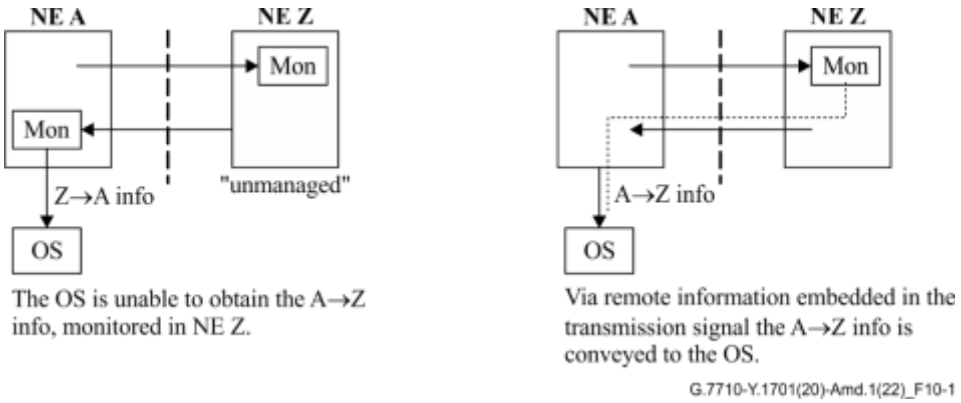


Figure ~~33~~10-1 – Single-ended maintenance through far-end monitoring

The left-hand side of Figure ~~33~~ 10-1 shows the unmanaged NE Z, whose measurements are inaccessible by the OS. The right-hand side shows the case where NE Z relays back its results (known as remote or backward information) to NE A. This backward information is post-processed (known as far-end monitoring) by NE A. The far-end monitoring results are accessible by the OS.

Related to the previously mentioned measurements, far-end monitoring is possible for BBE as the backward information contains the number of EBs (REI, BEI). Far-end monitoring is also possible for SES as the backward information contains an indication of a detected defect (RDI, BDI). Far-end monitoring for PJE is not possible as there is no backward information defined for these events.

10.1.2 Maintenance

The fault management supervision and validation processes (see clauses 7.1.1 and 7.1.2) describe an effective method to detect and analyse disturbances, and to provide an appropriate indication of the fault condition to maintenance personnel. The described processes, however, are not able to detect and report all causes leading to degraded performance. Maintenance measurements are required to detect additional error causes.

– In order to be able to do preventive maintenance, it is required to perform signal quality trend analysis. When the quality appears degraded, maintenance personnel may be instructed to replace or repair the degraded equipment before a failure is declared. Signal quality trend analysis is performed on signal quality maintenance measurements at the sink function.

  - For circuit layer: These measurements are based on transmitted block count (TBC), errored block count (EBC), block delay (BD) and calculated errored block ratio (EBR = EBC/TBC), background block count (BBC), background block errors (BBE) and block delay variation (BDV). A block is a set of consecutive bits – including an error detection code (EDC) – associated with the connection; each bit belongs to one, and only one, block. Consecutive bits may not be contiguous in time. An errored block (EB) is a block with one or more EDC violations. A BBE is an EB not occurring as part of a severely errored second (SES, see below). A background block (BB) is a transmitted block (TB) not occurring as part of an SES. The number of BBEs and BBs is summed over 15-minute and 24-hour intervals, over which the trend analysis is performed. The TBC is a circuit signal type and bit rate dependent, fixed value. Summary statistics (such as minimum, average, and maximum) for BD and BDV are derived over 15-minute and 24-hour interval for continuous monitoring.
  - For packet layer: These measurements are based on transmitted block count (TBC), lost block count (LBC), block delay (BD) and the calculated lost block ratio (LBR = LBC/TBC), background block count (BBC), background block error (BBE) and block delay variation (BDV). A block is a non-drop eligible frame or packet with a specific priority associated with the connection. An LB is a lost block. A BBE is a LB

not occurring as part of a severely errored second (SES). The number of BBEs is summed over 15-minute and 24-hour intervals, over which the trend analysis is performed. The TBC is a variable value. Summary statistics (such as minimum, average, and maximum) for BD and BDV are derived over 15-minute and 24-hour intervals for continuous monitoring.

– In order to locate the source of intermittent error conditions, e.g., short bursts of bit errors or lost frames or packets, it is required to measure these error conditions at various places in the network. These bursts cause a high EBR or LBR, or result in the declaration of framing defects (e.g., dLOF, dLOP). Fault management is not able to alert maintenance personnel in these cases because the defects do not persist long enough to become a failure.

  • Severely errored second (SES): The maintenance measurement is based on the detection of these bursts. An SES is declared when, during one second, the EBR or LBR exceeds a threshold, or when a defect is declared.

  The number of SESs is summed over 15-minute and 24-hour intervals. The analysis of these reports may be an aid to locate the error source.

– In order to determine whether the performance level is normal, degraded or unacceptable, it is required to set appropriate performance limits. For example, according to [ITU-T M.2101], the degraded and unacceptable performance limits are expressed as threshold values for the number of background block errors (BBEs), the number of errored seconds (ESs) and the number of SESs, summed over 15-minute intervals and 24-hour intervals. An ES is declared when, during one second, there are one or more EBs or LBs detected, or when a defect is declared. When a threshold report (see clause 10.1.7) is generated, maintenance personnel may be driven to perform additional network performance analysis.

– In order to locate the source that causes the generation of jitter and wander, e.g., due to a wrongly selected timing reference source, it is required to measure these error conditions. Jitter and wander can be measured directly by connecting the appropriate measurement equipment to the interface port. This method, however, may require maintenance personnel being present at the measurement location. An alternative approach, for example, is to measure the positive and negative pointer justification events (PJEs). These events may be an indication of a wrongly applied timing source. The PJEs are summed over 24-hour intervals. The analysis of these reports may be an aid to locate the error source.

– In order to locate equipment that needs adjustment or retuning, e.g., to limit drift or oscillation, it is required to do gauge measurements at or near the equipment. Examples of gauge measurements are the (optical) power level, the gain and the temperature. These gauges are measured periodically. Maintenance personnel may request a snapshot, in which case the current value is made available at the workstation or craft terminal. The NE keeps a record of the highest value and the lowest value of the gauge over 15-minute and 24-hour measurement intervals. The analysis of these gauge tidemark reports may drive maintenance personnel to readjust the equipment.

It must be noted that the previously described error causes are indeed detected by the indicated maintenance measurements. The reverse, however, is not always true: not every SES indicates a burst error; an increasing number of BBEs does not necessarily indicate degraded equipment; a large amount of PJEs need not be caused by a wrong timing reference source. Therefore, care must be taken with the analysis of the performance maintenance reports.

10.1.3 Bringing-into-service

Bringing-into-service (BIS) tests should be long-term measurements of new equipment, using a pseudo-random generator and receiver. However, for practical reasons the measurements may be reduced to a quick measurement and the assessment completed with in-service performance monitoring available in the network element. BIS methods for paths are defined in [ITU-T M.2110].

The BIS performance objectives for equipment supporting circuit layers, e.g., SDH paths, PDH paths, OTN ODU paths, etc., are based on the collection of ESs, SESs and BBEs. The BIS performance objectives for equipment supporting packet layers, e.g., ETH paths are based on the collection of ESs, SESs and BBEs or a subset of those. These measurements are evaluated in the management system and/or the NE over periods of 15 minutes, 2 hours, 1 day and 7 days. For the declaration of an SES, see the technology-specific ITU-T Recommendations, e.g., [ITU-T M.2101] defines the SDH BIS performance objectives in full detail.

The 15-minute and 24-hour registers should provide the capability to be reset to zero at the conclusion of the BIS intervals. If the history is stored as a log record, the capability to delete the log entries should be provided.

10.1.4 Quality of service

Quality of service (QoS) deals with service quality criteria stated in service provider specifications or service level agreements (SLAs) between service providers, or service providers and customers. In general, SLAs are applicable when there is a relationship, e.g., between a customer and an operator, or between a lead operator and several carriers. At a minimum, the SLA contains specifications for the grade of service to be delivered. Because of service provider specifications and SLA contracts, it is important for the service provider to measure the quality level during the "bringing the connection into service" phase. Once the NE and the connection is in service, both the service provider and the service customer need in-service performance measurements to validate the specifications or SLAs.

QoS measurements are performed once the NE and connections are in-service. These measurements cannot be PRBS-based, as the payload is reserved for the client signal. The QoS measurements are used to evaluate and validate the performance objectives to be met over an evaluation period of typically 30 consecutive days (one month). For example, Table ~~26~~10-1 lists the performance parameters used in SDH technology, defined in [ITU-T G.826], [ITU-T G.827], [ITU-T G.828] and [ITU-T G.829]. The right column specifies the measurements inside the NE.

Table ~~26~~10-1 – QoS performance parameters and NE measurements

Performance parameters	NE measurements (see Note)
Errored second ratio (ESR) is defined as the ratio of ESs in available time to total seconds in available time during a fixed measurement interval.	The NE shall count the number of ESs during 24-hour intervals.
Severely errored second ratio (SESR) is defined as the ratio of SESs in available time to total seconds in available time during a fixed measurement interval.	The NE shall count the number of SESs during 24-hour intervals.
Background block error ratio (BBER) is defined as the ratio of BBEs in available time to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.	The NE shall count the number of BBEs during 24-hour intervals.
Severely errored period intensity (SEPI) is defined as the number of SEP events in available time, divided by the total available time in seconds during a fixed measurement interval. Note that another name for SEP is CSES period.	The consecutive severely errored second (CSES) period is defined as a sequence of between three to nine consecutive SESs. The sequence is terminated by a second, which is not an SES. The NE shall time-stamp and log the start of the CSES event.

Table ~~26~~10-1 – QoS performance parameters and NE measurements

Performance parameters	NE measurements (see Note)
The availability ratio (AR) is defined as the ratio of the total available time to the duration of the fixed measurement interval. The total available time in the 24-hour interval is calculated as the difference between the number of seconds in the 24-hour interval (i.e., 86'400) and the number of unavailable seconds.	The NE shall administer the total unavailable time in one or two methods. The first method counts the number of unavailable seconds (UAS) during 24-hour intervals. The second method logs the begin time (BUT) and end time (EUT) of unavailable periods.
The outage intensity (OI) is defined as the reciprocal of the average duration of available time during a fixed measurement interval. The outage intensity over a 30-day interval is calculated as the quotient of the number of unavailable periods in the 30-day interval and the total available time of the 30-day interval.	As for the AR, the NE shall log the BUT and EUT.
NOTE – The NE measurements outlined here are only for QoS purposes. The full list and measurement intervals are to be found in clause 10.1.6.1.	

For QoS purposes, not only the measurements themselves are of importance, but also the locations where these measurements are done. As for maintenance measurements, described in clause 10.1.2, it is important to supervise both directions of the signal transmission from a single end of the connection. QoS measurements are also needed at any intermediate point of the connection. This is of particular importance if the lead operator is in the middle of the connection without management access to the end points.

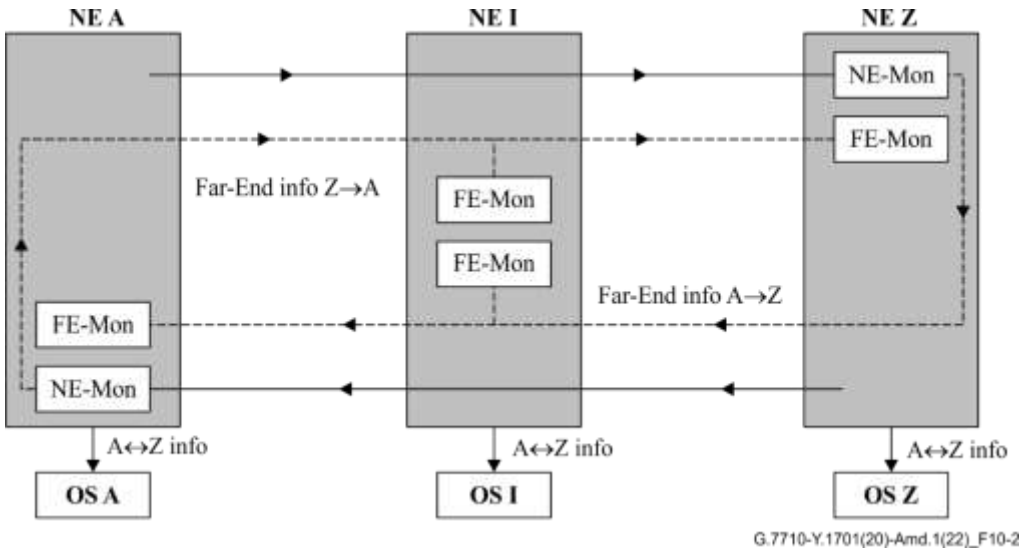


Figure ~~34~~10-2 – Single point QoS measurements

Figure ~~34~~ 10-2 outlines the bidirectional connection A-Z, passing an intermediate node I. The three NEs A, I and Z have, independently, the capability to supervise the bidirectional connection. In NE A, the near-end monitor (NE-Mon) and far-end monitor (FE-Mon) calculate the performance parameters of the Z→A and A→Z respectively. Likewise, in NE Z the NE-Mon and FE-Mon calculate the A→Z and Z→A parameters. In NE I there are two FE-monitors. The upper one in Figure ~~34~~ 10-2 is connected to the A→Z signal and monitors non-intrusively its far-end information, being Z→A. The lower one monitors non-intrusively the far-end A→Z information. In this way all three independent

NEs, and their independent management systems, are able to do bidirectional QoS measurements for the A↔Z connection.

10.1.5 Availability

The previous definitions are based on the concept of available time, which is defined as follows:

– A period of unavailable time begins at the onset of *x* consecutive SES events. These *x* seconds are considered to be part of unavailable time. A new period of available time begins at the onset of *x* consecutive non-SES events. These *x* seconds are considered to be part of available time. SEP indicates a severe error condition, which does not result in unavailability.

Figure ~~35~~ 10-3 illustrates the definition of criteria for SDH technology for transition to/from the unavailable state, including the relationship with SEP. For further details, see [ITU-T G.826] and [ITU-T G.828]. It must be noted that for the SDH case, *x* = 10.

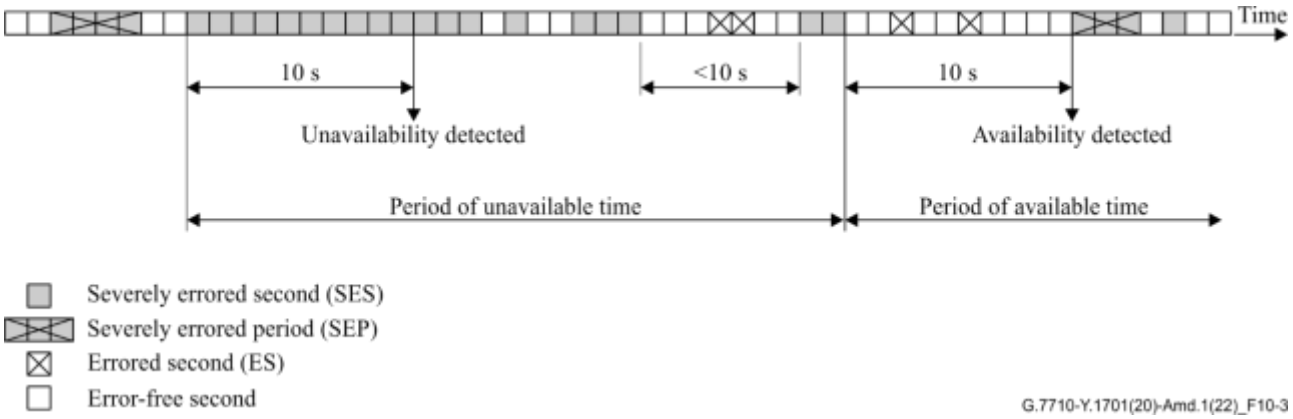


Figure ~~35~~ 10-3 – SDH example of unavailability determination

A bidirectional connection is in the unavailable state if either one, or both directions, are in the unavailable state. This is shown in Figure ~~36~~10-4. A unidirectional connection is in the unavailable state if that direction is in the unavailable state.

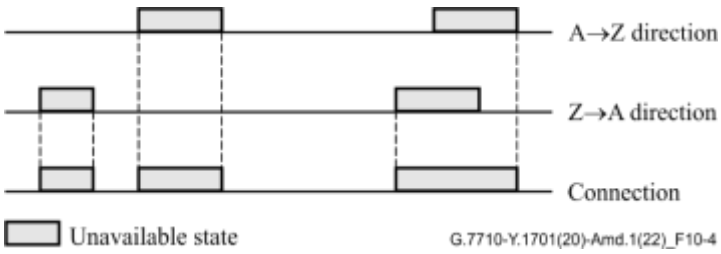


Figure ~~36~~ 10-4 – Example of the unavailable state of a bidirectional connection

10.1.6 Reporting

10.1.6.1 Performance data collection

Table ~~27~~10-2 summarizes the performance parameters the NE is able to collect for maintenance and quality of service purposes. This data is reported to the OS.

Table ~~27~~10-2 – Performance data collection

		Maintenance (each direction of the transport independently)	**Quality of service (Note 1)** (both directions of the transport together)
counts	15-minute interval 1 current + 16 recent (Note 2)	ES, SES, BBE, BBC, UAS	
	24-hour interval 1 current + 1 recent	ES, SES, BBE, BBC, UAS, PJE	ES, SES, BBE, BBC, SEP, UAS
events			BUT, EUT, CSES
snapshots	15-minute interval 1 current + 16 recent (Note 2)	gauge value at uniform time	
	24-hour interval 1 current + 1 recent	gauge value at uniform time	
tidemarks	15-minute interval 1 current + 16 recent (Note 2)	gauge highest value, gauge lowest value	
	24-hour interval 1 current + 1 recent	gauge highest value, gauge lowest value	
NOTE 1 – This is intended for bidirectional connections. For the case of unidirectional services, the other direction is not taken into account. NOTE 2 – The North American region may require 32 recent registers for 15-minute measurements. NOTE 3 – The technology-specific Recommendations may require only a subset of the performance parameters listed in the table.			

15-minute counts

The performance measurements are counted in a counter per measurement. These counters are called current registers.

It will be possible to reset an individual current register to zero by means of an external command. It will be possible to reset a collection of near-end and/or far-end registers (BBE, BBC, ES, SES, UAS) via one configuration command on a per TP basis or a group of TPs of the same type. If the TP performs bidirectional monitoring, the bidirectional UAS register shall be reset to zero when either the near-end group or the far-end group registers are reset to zero.

When history data storage is required, at the end of a 15-minute period, the contents of the current registers are transferred to the first of 16 recent registers, provided that the content is not zero and history storage suppression is not activated. After the transfer to the recent register, the current register shall be reset to zero. When all recent registers are used, the oldest information will be discarded. When history storage suppression (see clause 10.1.6.2) is activated, no transfer to the recent registers takes place when the current register contents are zero.

24-hour counts

The performance measurements are counted in a counter per measurement, independent of the 15-minute counters. These counters are called the current registers. It is up to the NE implementation when to update the register counts. It is not required to be done on a second-by-second basis, e.g., it is allowed to use the 15-minute register values to feed the 24-hour counts (for unidirectional connections only).

It will be possible to reset an individual current register to zero by means of an external command. It will be possible to reset a collection of near-end and/or far-end registers (BBE, BBC, ES, SES, UAS) via one configuration command on a per TP basis or a group of TPs of the same type. If the TP performs bidirectional monitoring, the bidirectional UAS register shall be reset to zero when either the near-end group or the far-end group registers are reset to zero.

When history storage is required, at the end of a 24-hour period, for each monitoring event, the contents of the current register are transferred to the recent register, provided that the content is not zero and history storage suppression is not activated. After the transfer to the recent register, the current register shall be reset to zero. When history storage suppression (see clause 10.1.6.2) is activated, no transfer to the recent register takes place when the current register contents are zero.

Events

The performance monitoring events, designated to be logged, are the begin unavailable time (BUT) event, the end unavailable time (EUT) event, and the time-stamped CSES event.

15-minute snapshot

The gauge measurements are stored in a register per measurement once, at a uniform time, within the 15-minute interval (a snapshot). These registers are called current registers.

At the end of a 15-minute period, the contents of the current registers are transferred to the first of 16 recent registers; the current register shall preserve its value. When all recent registers are used, the oldest information will be discarded. For specific applications, historical data may not be stored, e.g., only when threshold reports (see clause 10.1.7) are used, or when history storage suppression (see clause 10.1.6.2) is activated.

24-hour snapshot

The gauge measurements are stored in a register per measurement once, at a uniform time, within the 24-hour interval (a snapshot). These registers are called current registers.

At the end of a 24-hour period, for each gauge, the contents of the current register are transferred to the recent register; the current register shall preserve its value. For specific applications, historical data may not be stored, e.g., only when threshold reports (see clause 10.1.7) are used, or when history storage suppression (see clause 10.1.6.2) is activated.

15-minute tidemarks

Gauges are measured periodically within the 15-minute interval. The current 15-minute high tidemark register will contain the maximum value achieved, so far, by the gauge during the 15-minute interval. The current 15-minute low tidemark register will contain the minimum value achieved, so far, by the gauge during the 15-minute interval.

At the end of a 15-minute period, the contents of the current registers are transferred to the first of 16 recent registers; the current register will be reset to the current gauge value. When all recent registers are used, the oldest information will be discarded. For specific applications, historical data may not be stored, e.g., only when threshold reports (see clause 10.1.7) are used, or when history storage suppression (see clause 10.1.6.2) is activated.

24-hour tidemarks

Gauges are measured periodically within the 24-hour interval. The current 24-hour high tidemark register will contain the maximum value achieved, so far, by the gauge during the 24-hour interval. The current 24-hour low tidemark register will contain the minimum value achieved, so far, by the gauge during the 24-hour interval.

At the end of a 24-hour period, for each tidemark, the contents of the current register are transferred to the recent register; the current register shall be reset to the current gauge value. For specific

applications, historical data may not be stored, e.g., only when threshold reports (see clause 10.1.7) are used, or when history storage suppression (see clause 10.1.6.2) is activated.

Gauge measurement

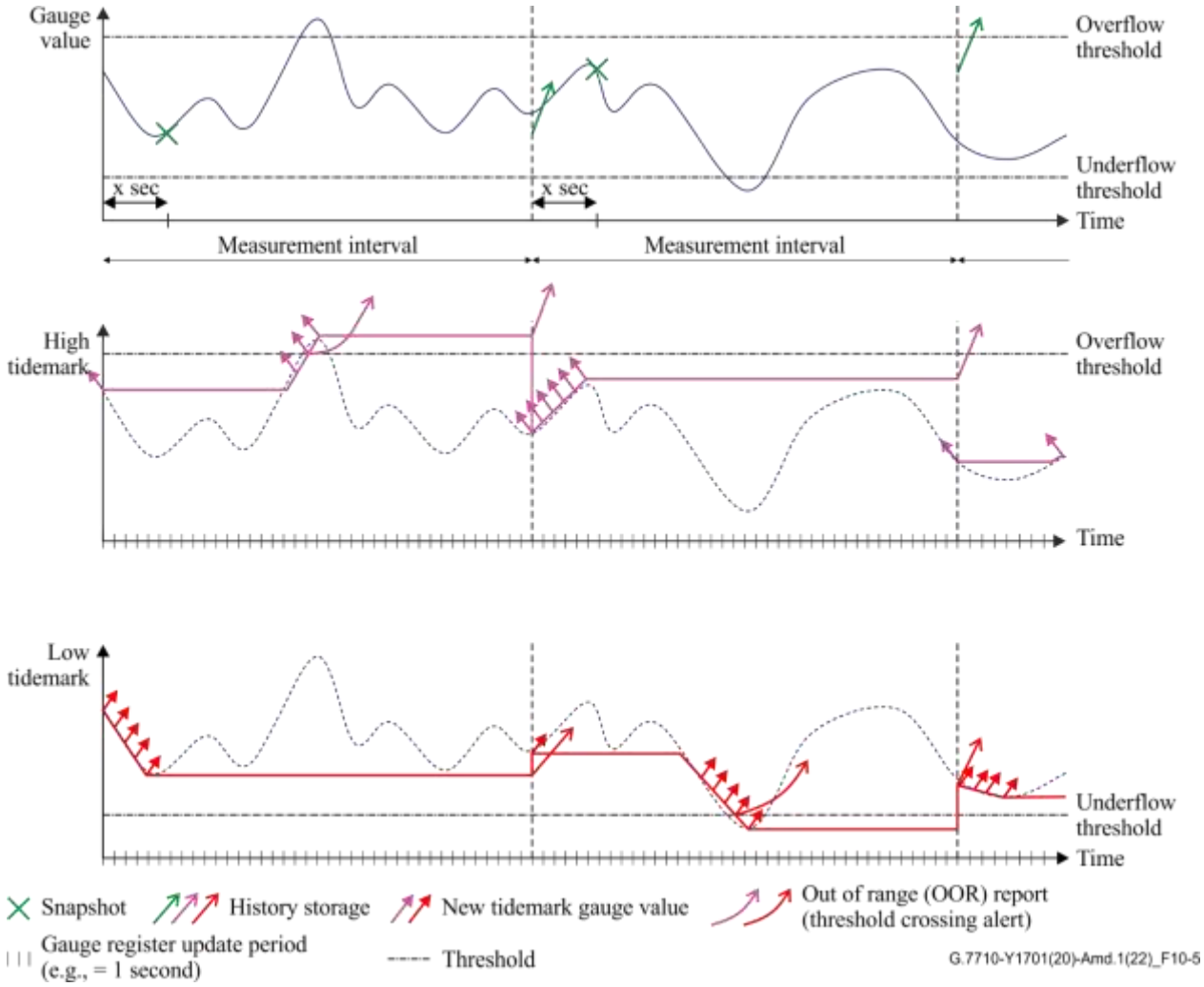


Figure ~~37~~ 10-5 – Gauge measurement

For each measurement interval, the gauge measurement at every second is used to update the high tidemark and low tidemark. If this update results in a new high tidemark and/or new low tidemark, the new high/low tidemark will be compared with the corresponding threshold value. For the 15-min (or 24-hr) snapshot, the gauge measurement is taken uniformly once per 15-min (or 24-hr).

Register attributes

The recent registers include a *time-stamp* attribute to indicate the end of the measurement interval.

The current and recent registers, holding counter values, include the *elapsed time* attribute to indicate how many seconds of the interval have been processed (so far). The elapsed time attribute will be initialized to zero at the start of the current interval. The nominal value of the elapsed time attribute is 900 s for a 15-minute interval, and 86'400 s for a 24-hour interval. Deviations to the nominal value can be caused by the following occurrences:

– The register belongs to the first (last) interval of the measurement, while the measurement did not start (stop) at an interval boundary.

– The start of the new interval is not exactly 900 s (or 86'400 s) later than the start of the current interval (see clause 8.13.1.1).

– The real-time clock makes a time adjustment caused by the alignment with an external time source (see clause 8.13.2.2).
– An outage condition prevents the collection of performance data, e.g., lost PM data in equipment.
– An incoming alignment error (IAE) event suppresses the performance data collection for the current and previous second. IAE does not stop the elapsed time counter.

The current and recent registers include a *suspect interval flag* to indicate that the performance data may not be reliable. Some reasons for this occurring are:

– The register belongs to the first or last interval of the measurement.
– The register belongs to an interval during which the measurement is suspended or resumed.
– The current register, designated for a counter, is reset by an external command.
– The recent register, designated for a counter, holds an elapsed time attribute value, which deviates more than 10 s with the nominal value.
– The register, designated for a snapshot or tidemark, contains no data, e.g., due to outage conditions.
– The register, designated for a tidemark, belongs to an interval during which the periodical gauge measurements are not possible, e.g., due to outage conditions.

[ITU-T Q.822] contains more examples of conditions that raise the suspect flag.

10.1.6.2 History storage suppression

History storage suppression deals with the limited storage of performance data in the MIB.

For counts this mechanism is known as zero suppression. Zero suppression is described in [ITU-T Q.822].

Zero suppression is defined as follows:

– any 15-minute or 24-hour period in which all collected data is equivalent to zero; and
– the invalid data/suspect flag is not set.

Other behaviours to note:

– When the 15-minute or 24-hour period completes the period, the data is checked.
– If no measurement occurred for a period (e.g., performance monitoring turned-off/locked, performance monitoring disabled, resource monitoring controlled by port mode), then the current data values are undefined and history records are not created at the end of period.

NOTE – Port mode is applicable only to SDH and PDH and superseded for new development (e.g., OTN). See Appendix III.

– Transitions to/from the 'locked' state and transitions to/from the 'disabled' state cause a current period to be marked invalid/suspect.

The history storage suppression mechanism for gauges is for further study.

By applying history storage suppression, the effective history storage capacity would be larger than 4 hours (i.e., 16 recent registers of 15 minutes each), as it can be expected that the majority of the counts will be zero. Another advantage is the limited history data transfer over the Q-interface.

10.1.7 Thresholding

A thresholding mechanism can be used to generate an autonomous event report when the performance of a transport entity falls outside a predetermined level. The general strategy for the use of thresholds, described in [ITU-T M.20], is based on the statistical analysis of performance parameters throughout

a given time. As soon as the result of the analysis reaches, or exceeds, a defined threshold, the entity is declared to be at an unacceptable level of performance, or at a degraded level of performance.

Thresholding for maintenance-based performance parameters is within the scope of this Recommendation. The results of the short-term analysis throughout the evaluation periods (15-minute and 24-hour) are reliable enough to declare the unacceptable (15-minute) or degraded (24-hour) level of performance. It must be noted that additional longer-term analysis for maintenance purposes may be required at the OSs. Thresholding for QoS-based performance parameters is outside the scope of this Recommendation because the statistical analysis throughout the evaluation period (typically 30 days) would require too much data storage capacity in the NE.

10.1.7.1 Threshold setting

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

10.1.7.2 Threshold reporting

Three basic methods of threshold reporting are defined:

The transient condition method treats each measurement period separately. As soon as a threshold is reached or crossed in a 15-minute/24-hour period, for a given performance measurement, a threshold report (TR) is generated. The transient condition method is applicable for counter measurements.

The standing condition method is an option for 15-minute periods. The standing condition is raised, and a TR is generated, when the set threshold is reached or crossed. The standing condition is cleared, and a reset threshold report (RTR) is generated, when at the end of the period the current value is below or equal to the reset threshold, provided that there was no unavailable time during that period. The standing condition method is applicable for counter measurements.

The out of range methods are like the transient condition method, but applicable for gauge measurements. For snapshots and high tidemarks, an overflow condition is determined and an out of range report (ORR) is generated as soon as the gauge value reaches or crosses the threshold. Likewise, for snapshots and low tidemarks, an underflow condition is determined and an out of range report (ORR) is generated as soon as the gauge value is at or below the threshold. The out of range methods are applicable for 15-minute and 24-hour measurements.

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

Refer to [ITU-T M.2120] for counter measurements; refer to [b-ANSI T1.231] for gauge measurements.

10.1.7.3 Evaluation for counters

During each 15-minute period, the value of the counter is compared to the set threshold on a second-by-second basis. For 24-hour periods, the NE shall recognize a threshold crossing within 15 minutes of its occurrence.

10.1.7.4 Evaluation for gauges

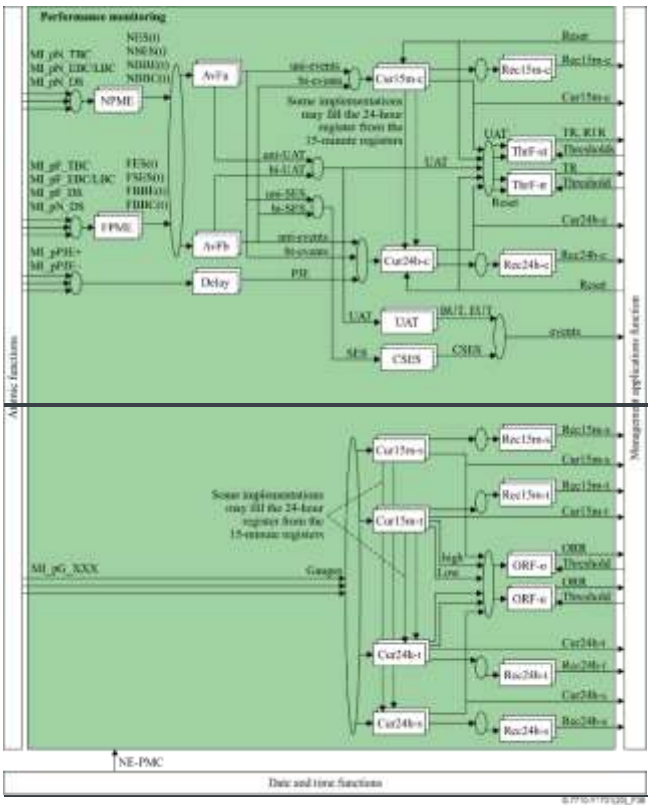
During each 15-minute period, the value of the gauge is compared to the set threshold at the moment a new gauge value becomes available. For 24-hour periods, the NE shall recognize a threshold crossing within 15 minutes of its occurrence.

10.2 Performance monitoring functions

Figure ~~38~~ 10-6 contains the functional model of performance monitoring inside the EMF. The white boxes are the performance monitoring functions (PMFs). Full specifications of the functions are given in subsequent clauses. The intermediate ellipses represent the interconnect options between the PMFs.

The equipment functional specification defines which (sub) set of PMFs is (to be) supported by the equipment, as well as the quantity of each PMF. For the case where the number of transport atomic functions exceeds the number of performance monitoring resources, selection may be indicated by "performance monitoring connection functions", or by alternative means. This is outside the scope of this Recommendation. For the case where such selectivity is not present or is not required, the interconnection is predefined and can be represented by explicit interconnections between PMFs and atomic functions.

Although Figure ~~38~~ 10-6 allows all possible interconnections, it must be noted that the performance monitoring packages, defined by the technology-specific Recommendations, determine which interconnections are applicable.


Performance monitoring
NE(n)
NM(n)
NBBE(n)
NBBC(n)
MI_pN_TBC
MI_pN_EBC/LBC
MI_pN_DS
NPME
AvFa
Some implementations may fill the 24-hour register from the 15-minute registers
Reset
Rec15m-c
Cur15m-c
UAT
TR, RTR
Threshold
TR
Threshold
ThrF-st
ThrF-e
Reset
Cur24h-c
Rec24h-c
Reset
FE(n)
FE/S(n)
FBBE(n)
FBBC(n)
MI_pF_TBC
MI_pF_EBC/LBC
MI_pF_DS
FPME
AvFb
MI_pPH+
MI_pPH-
Delay
PH
UAT
UAT
SES
CSES
SES, UAT, CSES
events
Some implementations may fill the 24-hour register from the 15-minute registers
Rec15m-s
Cur15m-s
Rec15m-t
Cur15m-t
MI_pG_XXX
Gauges
high
Low
ORF-e
ORF-e
ORR
Threshold
ORR
Threshold
Cur24h-t
Rec24h-t
Cur24h-s
Rec24h-s
Atomic functions
Management application function
NE-PMC
Data and time functions

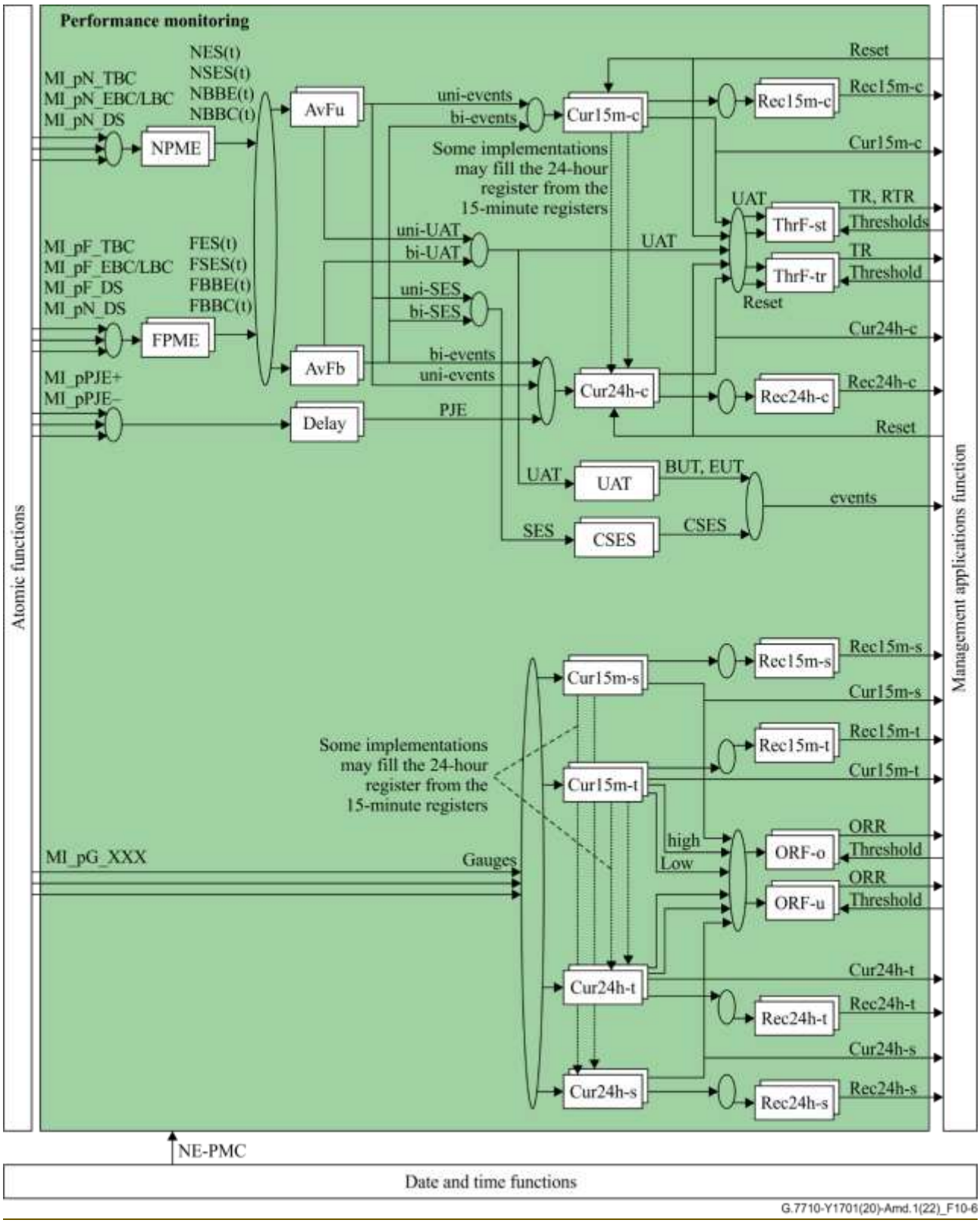


Figure ~~38~~10-6 – Performance monitoring inside the EMF

10.2.1 Near-end performance monitoring event function – NPME

Symbol:

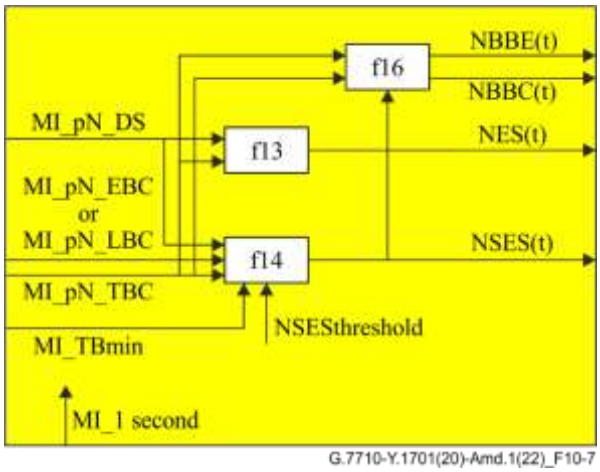


Figure ~~39~~10-7 – NPME

Interfaces:

Table ~~28~~10-3 – NPME input and output signals

Input(s)	Output(s)
MI_pN_DS MI_pN_EBC or MI_pN_LBC MI_pN_TBC MI_1second MI_TBmin NSESthreshold	NBBE(t) NBBC(t) NES(t) NSES(t)

Processes:

This function determines, on a per second basis, the number of near-end background block errors (BBE), near-end background block count, and whether an ES and/or SES occurred.

The TBC, EBC or LBC, and DS performance monitoring primitive signals received from a transport atomic function, are the inputs for the determination of the performance events BBE, BBC, ES, SES.

For the case where a DS input is not connected, DS shall be assumed to be false. In the case where an EBC input is not connected, EBC shall be assumed to be "0". In the case where a TBC input is not connected, TBC shall be assumed to be "1".

Figure ~~39~~ 10-7 presents the processes and their interconnections within the near-end performance monitoring event (NPME) atomic performance monitoring function.

f13: A near-end errored second (NES) performance monitoring event signal shall be generated if pN_DS is set or if pN_EBC ≥ 1; i.e.:

– NES ← (pN_DS = true) or (pN_EBC ≥ 1).

f14: A near-end severely errored second (NSES) performance monitoring event signal shall be generated if pN_DS is set or if pN_EBC (or pN_LBC) ≥ NSESthreshold × pN_TBC and more than a minimum number of blocks (TBmin) were transmitted; i.e.:

– NSES ← (pN_DS = true) or ((pN_TBC ≥ TBmin) and (pN_EBC or pN_LBC ≥ NSESthreshold × pN_TBC)).

The value of the near-end SES threshold, NSESthreshold, depends on the network layer this NPME is connected to. The value of NSESthreshold is a real value between 0 and 1.

NOTE – For circuit layers (SDH, PDH, OTN) where the number of blocks within a one-second period is a fixed known value, pN_TBC is representing this fixed known value. For packet layers (e.g., ETH) where the number of blocks (i.e., frames or packets) within a one-second period is variable, pN_TBC represents the counted number of transmitted blocks within the one-second period.

f16: The near-end background block error (NBBE) and near-end background block count (NBBC) performance monitoring event signals shall equal pN_EBC and pN_TBC resp. if the NSES of that second is not set. Otherwise, NBBE and NBBC shall be zero.

10.2.2 Far-end performance monitoring event function – FPME

Symbol:

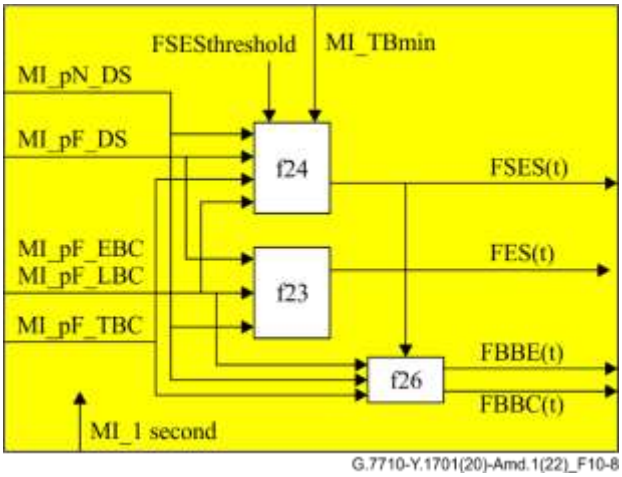


Figure ~~40~~10-8 – FPME

Interfaces:

Table ~~29~~10-4 – FPME input and output signals

Input(s)	Output(s)
MI_pN_DS MI_pF_DS MI_pF_EBC or MI_pF_LBC MI_pF_TBC MI_1second MI_TBmin FSESthreshold	FBBE(t) FBBC(t) FES(t) FSES(t)

Processes:

This function determines, on a per second basis, the number of far-end background block errors (BBE), far-end background block count, and whether an ES and/or SES occurred.

The TBC, EBC or LBC, and DS performance monitoring primitive signals received from an atomic function are the inputs for the determination of the performance events BBE, BBC, ES, SES.

In the case where a DS input is not connected, DS shall be assumed to be false. For the case an EBC input is not connected, EBC shall be assumed to be "0". In the case where a TBC input is not connected, TBC shall be assumed to be "1".

Figure ~~40~~ 10-8 presents the processes and their interconnections within the far-end performance monitoring event (FPME) atomic performance monitoring function. Note that "far-end" represents either those signals that are called "far-end" or those signals that are called "outgoing".

f23: A far-end errored second (FES) performance monitoring event signal shall be generated if pF_DS is set or if pF_EBC ≥ 1, and if that second is not a near-end defect second (pN_DS); i.e.:

– FES ← (pN_DS = false) and ((pF_DS = true) or (pF_EBC ≥ 1)).

f24: A far-end severely errored second (FSES) performance monitoring event signal shall be generated if pF_DS is set or if pF_EBC (or pF_LBC) ≥ FSESthreshold × pF_TBC and more than a minimum number of blocks (TBmin) were transmitted, and that a second is not a near-end defect second; i.e.:

– FSES ← (pN_DS = false) and ((pF_DS = true) or ((pN_TBC ≥ TBmin) and (pF_EBC or pF_LBC ≥ FSESthreshold × pF_TBC)).

The value of the far-end SES threshold, FSESthreshold, depends on the network layer this FPME is connected to. The value of FSESthreshold is a real value between 0 and 1.

NOTE – For circuit layers (SDH, PDH, OTN) where the number of blocks within a one-second period is a fixed known value, pF_TBC is representing this fixed known value. For packet layers (e.g., ETH) where the number of blocks (i.e., frames or packets) within a one-second period is variable, pF_TBC represents the counted number of transmitted blocks within the one-second period.

f26: The far-end background block error (FBBE) and far-end background block count (FBBC) performance monitoring event signal shall equal pF_EBC and pF_TBC resp. if the FSES of that second is not set and if that second is not a near-end defect second. Otherwise, FBBE and FBBC shall be zero.

10.2.3 Delay function – Delay

Symbol:

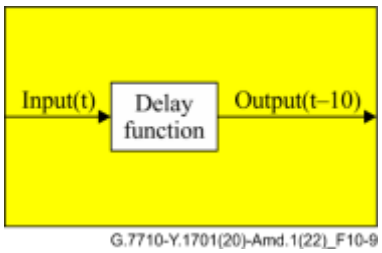


Figure ~~41~~ 10-9 – Delay

Interfaces:

Table ~~30~~ 10-5 – Delay input and output signals

Input(s)	Output(s)
Input(t)	Output(t–10)

Processes:

This function delays the input signal (which is not subject to "availability" processing) by 10 s to align it with the performance monitoring time base which is 10 s delayed from the time of day.

Delay function: The input signal (e.g., PJE) shall be delayed by 10 s to align it with the performance monitoring time base signal for further processing in the history atomic performance monitoring functions.

10.2.4 Unidirectional availability filter function – AvFu

Symbol:

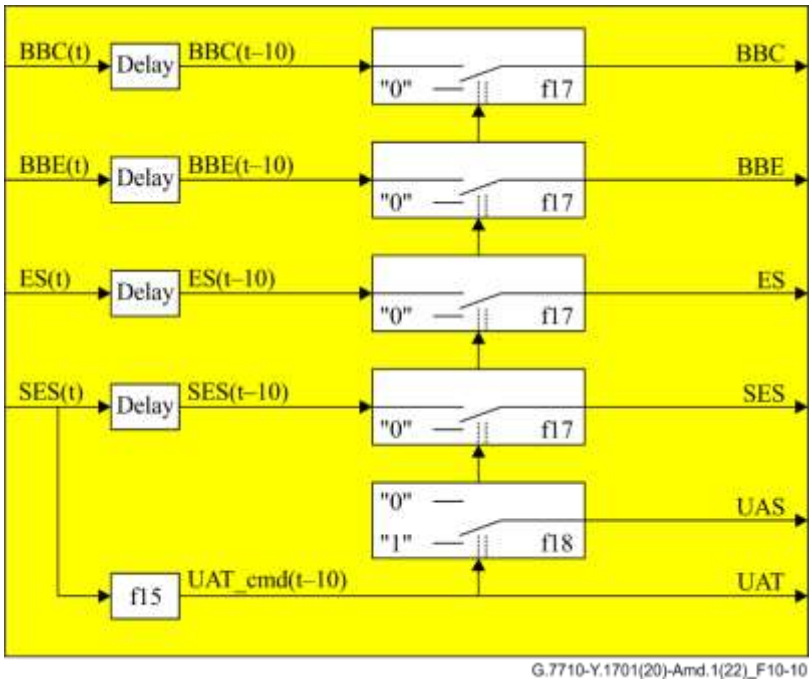


Figure ~~42~~ 10-10 – AvFu

Interfaces:

Table ~~31~~10-6 – AvFu input and output signals

Input(s)	Output(s)
BBE(t) BBC(t) ES(t) SES(t)	BBE BBC ES SES UAS UAT

Processes:

This function determines whether a one second is unidirectionally available or unavailable, and passes through the (ES, SES, BBE, BBC) input signal's value for seconds in available time. The input signal value in seconds in unavailable time is not output; instead the value "0" is output. This function is applicable for near-end, far-end, near-end outgoing and far-end outgoing information processing.

Based on the SES event indications, the start and end of UAT is determined. The BBE, BBC, ES and SES information is delayed by 10 s to maintain alignment in time of this information and the UAT indication (UATcmd).

For the case where the BBE(t) input is not connected, BBE(t) shall be assumed to be "0". For the case where the BBC(t) input is not connected, BBC(t) shall be assumed to be "0". In the case where the ES(t) input is not connected, ES(t) shall be assumed to be "0". In the case where the SES(t) input is not connected, SES(t) shall be assumed to be "0".

f15: Unavailable time command (UAT_cmd) shall be set if ten consecutive SESs are detected. UAT_cmd shall be cleared after ten contiguous seconds not being SES.

A change of the UAT_cmd shall be reported.

delay: The BBE, BBC, ES and SES event signals shall be delayed by 10 s to align them with the UATcmd signal for further processing in the history atomic performance monitoring functions (see also clause 10.2.3).

f17: The BBE(t–10), BBC(t–10), ES(t–10) and SES(t–10) event signals shall be output in available time; i.e., if UATcmd is false. Otherwise, the value "0" shall be output.

f18: In available time (i.e., if UATcmd is false), the value "0" shall be output via UAS. Otherwise (UATcmd is true), the value "1" shall be output.

10.2.5 Bidirectional availability filter function – AvFb

Symbol:

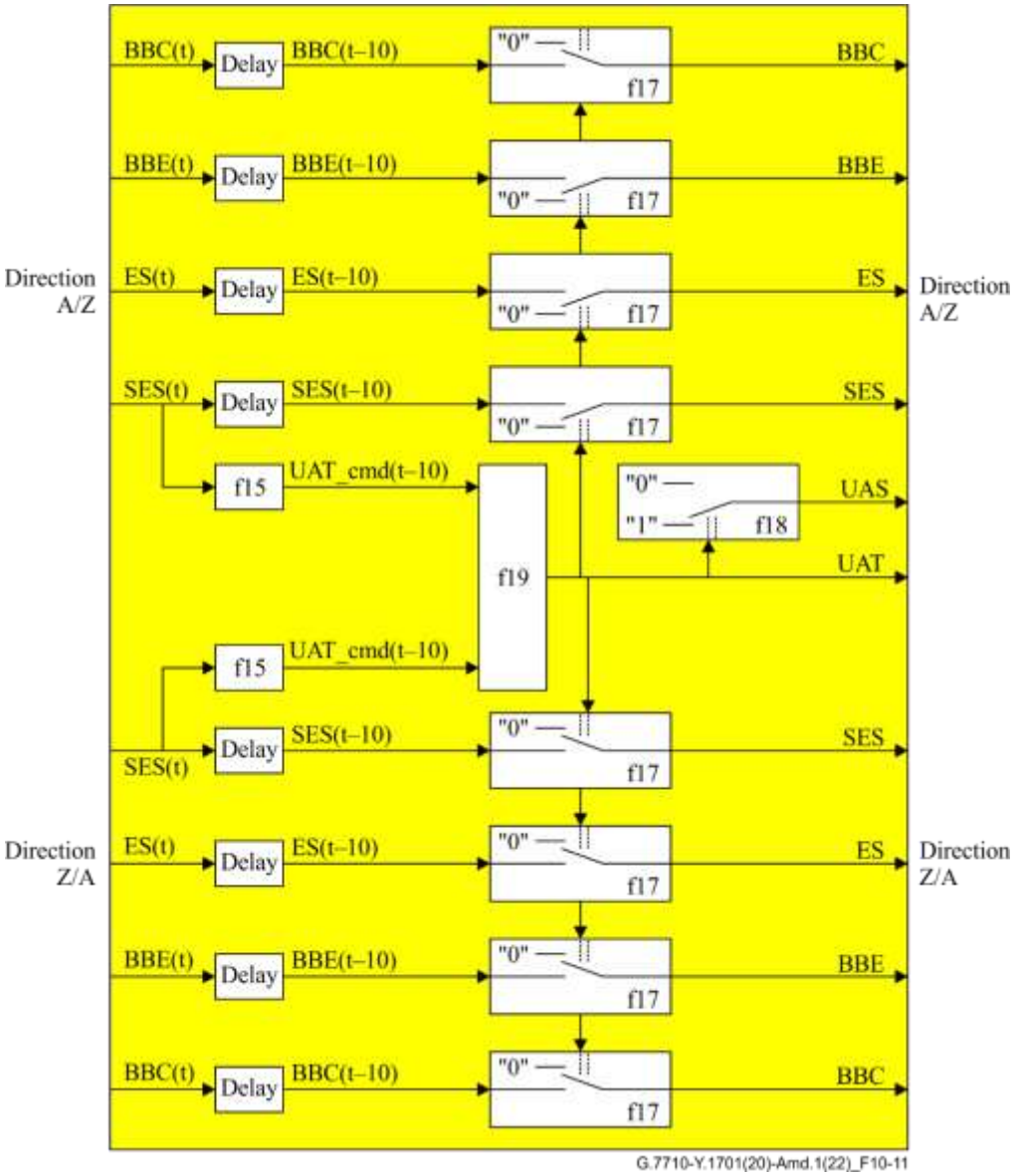


Figure ~~43~~ 10-11 – AvFb

Interfaces:

Table ~~32~~10-7 – AvFb input and output signals

Input(s)	Output(s)
A/Z_BBE(t) A/Z_BBC(t) A/Z_ES(t) A/Z_SES(t) Z/A_BBE(t) Z/A_ES(t) Z/A_SES(t) Z/A_BBC(t)	A/Z_BBE A/Z_BBC A/Z_ES A/Z_SES Z/A_BBE Z/A_BBC Z/A_ES Z/A_SES UAS UAT

Processes:

This function determines whether a one second is bidirectionally available or unavailable, and passes through the (ES, SES, BBE, BBC) input signal's value in seconds in available time. The input signal value in seconds in unavailable time is not output; instead the value "0" is output.

Based on the SES event indications, the start and end of UAT is determined. The BBE, BBC, ES and SES information is delayed by 10 s to maintain alignment in time of this information and the UAT indication (UATcmd). Note that the A/Z and Z/A direction indication is used here instead of the more common near-end and far-end indications to support performance monitoring at both the trail termination points and intermediate points along the trail.

In the case where the BBE(t) input is not connected, BBE(t) shall be assumed to be "0". In the case where the BBC(t) input is not connected, BBC(t) shall be assumed to be "0". In the case where the ES(t) input is not connected, ES(t) shall be assumed to be "0". In the case where the SES(t) input is not connected, SES(t) shall be assumed to be "0".

f15: Unavailable time command (UAT_cmd) shall be set if ten consecutive SESs are detected. UAT_cmd shall be cleared after ten contiguous seconds not being SES.

f19: Bidirectional unavailable time shall be declared if either the A/Z direction is unavailable or the Z/A direction is unavailable:

– UAT ← A/Z_UAT_cmd(t–10) or Z/A_UAT_cmd(t–10).

A change of the UAT shall be reported.

delay: The BBE, BBC, ES and SES signals are delayed by 10 s to align them with the UATcmd signal for further processing in the history atomic performance monitoring functions (see also clause 10.2.3).

f17: The BBE(t–10), BBC(t–10), ES(t–10) and SES(t–10) signals shall be output in available time; i.e., if UAT is false. Otherwise, the value "0" shall be output.

f18: In available time (i.e., if UAT is false), the value "0" shall be output via UAS. Otherwise (UAT is true), the value "1" shall be output.

10.2.6 Consecutive severely errored second function – CSES

Symbol:

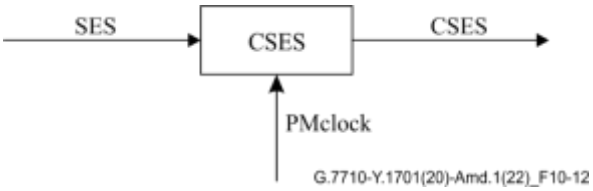


Figure ~~44~~10-12 – CSES

Interfaces:

Table ~~33~~ 10-8 – CSES input and output signals

Input(s)	Output(s)
SES PMclock	CSES

Processes:

This function detects a sequence of between 3 to 9 consecutive SESs. The sequence is terminated by a second, which is not an SES.

The function shall generate a time-stamped CSES event if three consecutive SESs are detected.

10.2.7 Begin/end of unavailable time event generation function – UAT

Symbol:

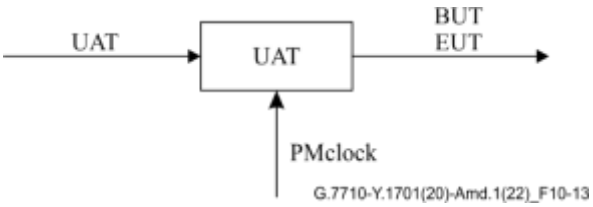


Figure ~~45~~ 10-13 – UAT

Interfaces:

Table ~~34~~ 10-9 – UAT input and output signals

Input(s)	Output(s)
UAT PMclock	BUT EUT

Processes:

This function detects the start and end of unavailable periods.

The function shall generate a time-stamped begin unavailable time (BUT) event if the UAT state changes from "available" to "unavailable". The function shall generate a time-stamped end unavailable time (EUT) event if the UAT state changes from "unavailable" to "available".

10.2.8 Current 15-minute counter register function – Cur15m-c

Symbol:

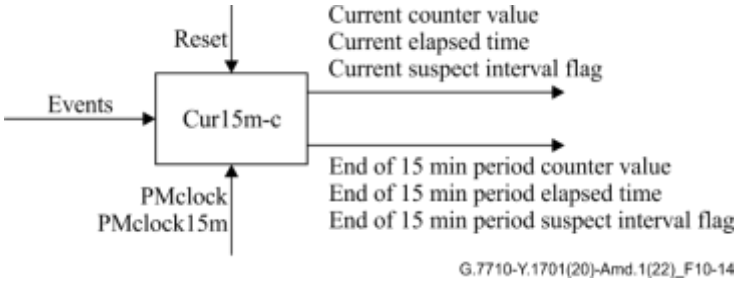


Figure ~~46~~ 10-14 – Cur15m-c

Interfaces:

Table ~~35~~ 10-10 – Cur15m-c input and output signals

Input(s)	Output(s)
Events PMclock PMclock15m Reset	Current counter value Current elapsed time Current suspect interval flag End of 15 min period counter value End of 15 min period elapsed time End of 15 min period suspect interval flag

Processes:

This function accumulates the events over periods of 15 minutes.

Current register counter value: The 15-minute current register shall accumulate the content of the register with the input events. The counter value shall be initialized to zero at the start of a new 15-minute interval. The current register shall be large enough to accumulate all integer numbers from zero to a particular maximum value, which determines the minimum register size for that parameter. The maximum value shall be at least the nominal count of an interval. When the maximum value of the register is reached, the register shall remain at that maximum value until it is reset, or transferred. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register counter value reset: By means of an external command, it shall be possible to reset the current register counter value to zero.

Current register elapsed time: The current register shall contain an elapsed time indication, indicating how many seconds of the interval have been processed (so far). The elapsed time attribute shall be initialized to zero at the start of the current interval. The current register elapsed time shall be able to indicate at least the elapsed time of the nominal interval; i.e., 900 s. When the maximum value of an elapsed time register is reached, the register shall remain at that maximum value until it is reset, or transferred.

Current register suspect interval flag: The current register suspect interval flag will be set to "true" to indicate that the data stored in the register may not be reliable. The suspect interval flag shall be initialized to "true" for the very first interval of the measurement. The suspect interval flag shall be initialized to "false" at the start of subsequent new 15-minute intervals. During the 15-minute interval period, the suspect flag shall be set when the current register counter value is reset to zero (see also "End of accumulation period").

Report current register: It shall be possible to report the value of the current register when requested.

End of accumulation period: At the end of the 15-minute accumulation period, the contents of the current register may be transferred to the recent register. Prior to the transfer, the suspect interval flag shall be set if the elapsed time deviates from more than 10 s of the nominal time, being 900 s. After the transfer, the current register shall be initialized. If the NE-RTC (and consequently the PMclock) is set to a time outside the current interval, the end of the 15-minute accumulation period shall be assumed, and the actions as specified above shall be performed.

10.2.9 Current 15-minute snapshot register function – Cur15m-s

Symbol:

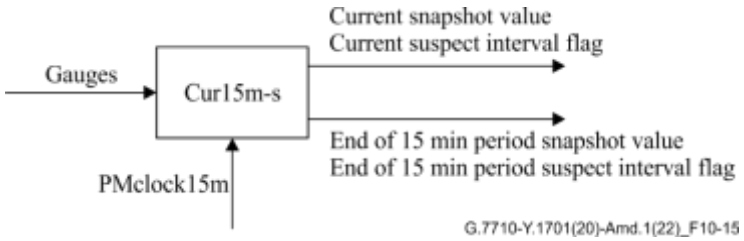


Figure ~~47~~ 10-15 – Cur15m-s

Interfaces:

Table ~~36~~ 10-11 – Cur15m-s input and output signals

Input(s)	Output(s)
Gauges PMclock15m	Current snapshot value Current suspect interval flag End of 15 min period snapshot value End of 15 min period suspect interval flag

Processes:

This function selects one gauge measurement as the current 15-minute snapshot.

Current register snapshot value: The 15-minute current register shall hold the value of one gauge measurement. The gauge measurement shall be selected at a uniform time within the 15-minute interval. The current register's snapshot value shall not be initialized at the start of a new 15-minute interval; instead, it preserves the snapshot value from the previous 15-minute interval. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register suspect interval flag: The current register suspect interval flag will be set to true to indicate that the data stored in the register may not be reliable. The suspect interval flag shall be initialized to "true" at the start of a 15-minute interval to indicate that no snapshot has been taken yet. The suspect interval flag shall be set to "false" after the snapshot has been taken.

Report current register: It shall be possible to report the value of the current register when requested.

End of accumulation period: At the end of the 15-minute accumulation period, the contents of the current register may be transferred to the recent register, after which the current register shall be initialized. If the NE-RTC (and consequently the PMclock) is set to a time outside the current interval, the end of the 15-minute accumulation period shall be assumed, and the actions as specified above shall be performed.

10.2.10 Current 15-minute tidemark register function – Cur15m-t

Symbol:

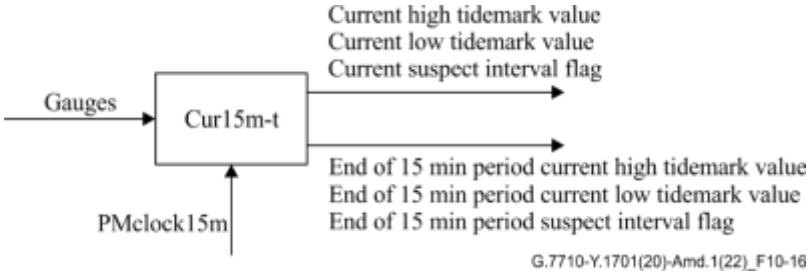


Figure ~~48~~ 10-16 – Cur15m-tidemark

Interfaces:

Table ~~37~~ 10-12 – Cur15m-t input and output signals

Input(s)	Output(s)
Gauges PMclock15m	current high tidemark value Current low tidemark value Current suspect interval flag End of 15 min period high tidemark value End of 15 min period low tidemark value End of 15 min period suspect interval flag

Processes:

This function registers the highest and lowest value of periodic gauge measurements during the current 15-minute interval.

Current register high tidemark value: The current 15-minute high tidemark register shall contain the maximum value achieved, so far, by the gauge during the 15-minute interval. The current register's high tidemark value shall be initialized to the instantaneous gauge value at the start of a new 15-minute interval. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register low tidemark value: The current 15-minute low tidemark register shall contain the minimum value achieved, so far, by the gauge during the 15-minute interval. The current register's low tidemark value shall be initialized to the instantaneous gauge value at the start of a new 15-minute interval. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register suspect interval flag: The current register suspect interval flag will be set to true to indicate that the data stored in the register may not be reliable. The suspect interval flag shall be initialized to "false" at the start of a 15-minute interval. During the 15-minute interval period, the suspect flag shall be set when there is a lack of periodic gauge measurements.

Report current register: It shall be possible to report the value of the current register when requested.

End of accumulation period: At the end of the 15-minute accumulation period, the contents of the current register may be transferred to the recent register, after which the current register shall be initialized. If the NE-RTC (and consequently the PMclock) is set to a time outside the current interval, the end of the 15-minute accumulation period shall be assumed, and the actions as specified above shall be performed.

10.2.11 Recent 15-minute register functions – Rec15m-c, Rec15m-s, Rec15m-t

Symbol:

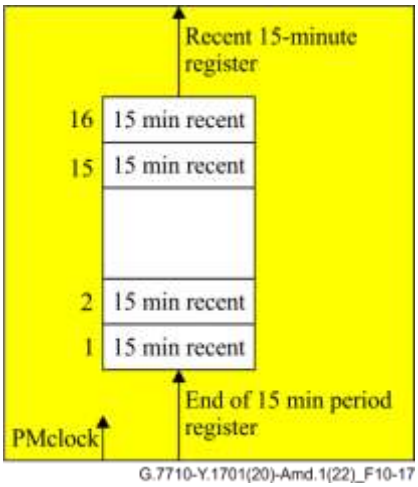


Figure ~~49~~ 10-17 – Rec15m-c, Rec15m-s, Rec15m-t

Interfaces:

Table ~~38~~ 10-13 – Rec15m-c, Rec15m-s, Rec15m-t input and output signals

Input(s)	Output(s)
End of 15 min period register PMclock	Recent 15 min register [1:16]

Functions/Processes:

The Rec15m-c function stores the end of 15-min period counter value, elapsed time and suspect interval flag in one of the 16 recent registers. The Rec15m-s function stores the end of 15-min period snapshot value and suspect interval flag in one of the 16 recent registers. The Rec15m-t function stores the end of 15-min period high tidemark value, low tidemark value and suspect interval flag in one of the 16 recent registers.

Recent registers: At the end of the 15-minute period, when history data storage is not suppressed, the end of 15-min period register input shall be transferred to the recent #1 register. Before the data is transferred, any data in the recent #i (i = 1…15) registers shall be transferred to the recent #(i+1) registers. The data in the recent#16 register shall be discarded.

Recent register time stamp: The recent register shall contain a time-stamp indicating the end of the recent interval.

Report recent register: It shall be possible to report the value of the recent registers when requested.

10.2.12 Current 24-hour counter register function – Cur24h-c

Symbol:

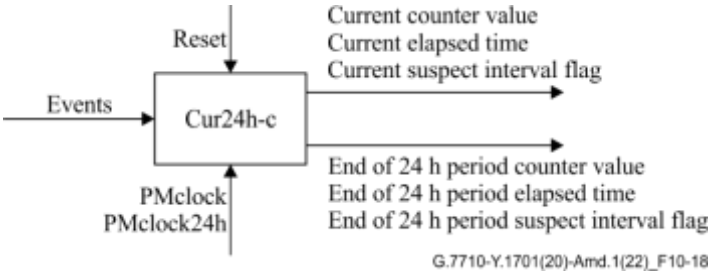


Figure ~~50~~ 10-18 – Cur24h-c

Interfaces:

Table ~~39~~ 10-14 – Cur24h-c input and output signals

Input(s)	Output(s)
Events PMclock PMclock24h	Current counter value Current elapsed time Current suspect interval flag End of 24 h period counter value End of 24 h period elapsed time End of 24 h period suspect interval flag

Processes:

This function accumulates the events over periods of 24 hours.

Current register counter value: The 24-hour current register shall accumulate the content of the register with the input events. The counter value shall be initialized to zero at the start of a new 24-hour interval. The current register shall be large enough to accumulate all integer numbers from zero to a particular maximum value, which determines the minimum register size for that parameter. The maximum value shall be at least the nominal count of an interval. When the maximum value of the register is reached, the register shall remain at that maximum value until it is reset, or transferred. Current data may be lost during failure conditions within the equipment and its power feeding.

NOTE 1 – Although all event counts should (ideally) be actual counts for the 24-hour filtering periods, it is recognized that it might be desirable to limit register sizes.

NOTE 2 – 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. An update once every 15 minutes would be sufficient.

Current register counter value reset: By means of an external command it shall be possible to reset the current register counter value to zero.

Current register elapsed time: The current register shall contain an elapsed time indication, indicating how many seconds of the interval have been processed (so far). The elapsed time attribute shall be initialized to zero at the start of the current interval. The current register elapsed time shall be able to indicate at least the elapsed time of the nominal interval; i.e., 86'400 s. When the maximum value of an elapsed time register is reached, the register shall remain at that maximum value until it is reset, or transferred.

Current register suspect interval flag: The current register suspect interval flag will be set to "true" to indicate that the data stored in the register may not be reliable. The suspect interval flag shall be initialized to "true" for the very first interval of the measurement. The suspect interval flag shall be initialized to "false" at the start of subsequent new 24-hour intervals. During the 24-hour interval period, the suspect flag shall be set when the current register counter value is reset to zero (see also "End of accumulation period").

Report current register: It shall be possible to report the value of the current register when requested.

End of accumulation period: At the end of the 24-hour accumulation period, the contents of the current register may be transferred to the recent register. Prior to the transfer, the suspect interval flag shall be set if the elapsed time deviates from more than 10 s of the nominal time, being 86 400 s. After the transfer, the current register shall be initialized. If the NE-RTC (and consequently the PMclock) is set to a time outside the current interval, the end of the 24-hour accumulation period shall be assumed, and the actions as specified above shall be performed.

10.2.13 Current 24-hour snapshot register function – Cur24h-s

Symbol:

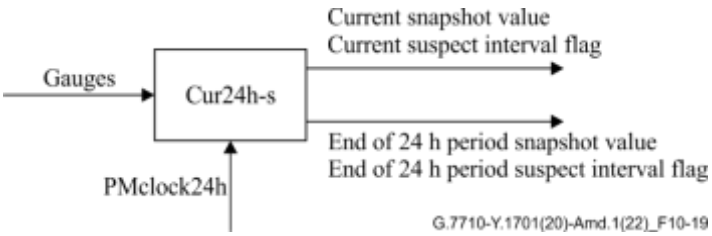


Figure ~~51~~ 10-19 – Cur24h-s

Interfaces:

Table ~~40~~10-15 – Cur24h-snapshot input and output signals

Input(s)	Output(s)
Gauges PMclock24h	Current snapshot value Current suspect interval flag End of 24 h period snapshot value End of 24 h period suspect interval flag

Processes:

This function selects one gauge measurement as a current 24-hour snapshot.

Current register snapshot value: The 24-hour current register shall hold the value of one gauge measurement. The gauge measurement shall be selected at a uniform time within the 24-hour interval. The current register's snapshot value shall not be initialized at the start of a new 24-hour interval; instead, it preserves the snapshot value from the previous 24-hour interval. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register suspect interval flag: The current register suspect interval flag will be set to "true" to indicate that the data stored in the register may not be reliable. The suspect interval flag shall be initialized to "true" at the start of a 24-hour interval to indicate that no snapshot has yet been taken. The suspect interval flag shall be set to "false" after the snapshot has been taken.

Report current register: It shall be possible to report the value of the current register when requested.

End of accumulation period: At the end of the 24-hour accumulation period, the contents of the current register may be transferred to the recent register, after which the current register shall be initialized. If the NE-RTC (and consequently the PMclock) is set to a time outside the current interval, the end of the 24-hour accumulation period shall be assumed and the actions, as specified above, shall be performed.

10.2.14 Current 24-hour tidemark register function – Cur24h-t

Symbol:

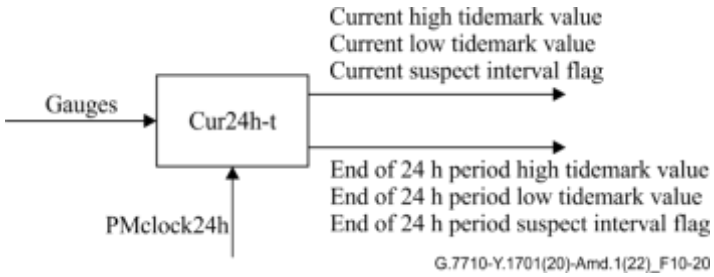


Figure ~~52~~ 10-20 – Cur24h-t

Interfaces:

Table ~~41~~ 10-16 – Cur24h-t input and output signals

Input(s)	Output(s)
Gauges PMclock24h	Current high tidemark value Current low tidemark value Current suspect interval flag End of 24 h period high tidemark value End of 24 h period low tidemark value End of 24 h period suspect interval flag

Processes:

This function registers the highest and lowest value of the periodic gauge measurements during the current 24-hour interval.

Current register high tidemark value: The current 24-hour high tidemark register shall contain the maximum value achieved, so far, by the gauge during the 24-hour interval. The current register's high tidemark value shall be initialized to the instantaneous gauge value at the start of a new 24-hour interval. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register low tidemark value: The current 24-hour low tidemark register shall contain the minimum value achieved, so far, by the gauge during the 24-hour interval. The current register's low tidemark value shall be initialized to the instantaneous gauge value at the start of a new 24-hour interval. Current data may be lost during failure conditions within the equipment and its power feeding.

Current register suspect interval flag: The current register suspect interval flag will be set to "true" to indicate that the data stored in the register may not be reliable. The suspect interval flag shall be initialized to "false" at the start of a 24-hour interval. During the 24-hour interval period, the suspect flag shall be set when there is a lack of periodic gauge measurements.

Report current register: It shall be possible to report the value of the current register when requested.

End of accumulation period: At the end of the 24-hour accumulation period, the contents of the current register may be transferred to the recent register, after which the current register shall be initialized. If the NE-RTC (and consequently the PMclock) is set to a time outside the current interval, the end of the 24-hour accumulation period shall be assumed, and the actions as specified above shall be performed.

10.2.15 Recent 24-hour register functions – Rec24h-c, Rec24h-s, Rec24h-t

Symbol:

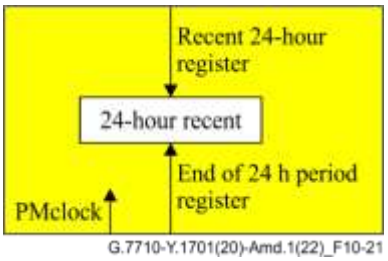


Figure ~~53~~ 10-21 – Rec24h-c, Rec24h-s, Rec24h-t

Interfaces:

Table ~~42~~ 10-17 – Rec24h-c, Rec24h-s, Rec24h-t input and output signals

Input(s)	Output(s)
End of 24 h period register PMclock	Recent 24 h register

Functions/Processes:

The Rec24h-c function stores the end of 24-hour period counter value, elapsed time and suspect interval flag in the recent register. The Rec24h-s function stores the end of 24-hour period snapshot value and suspect interval flag in the recent register. The Rec24h-t function stores the end of 24-hour period high tidemark value, low tidemark value and suspect interval flag in the recent register.

Recent register: At the end of the 24-hour period, when history data storage is not suppressed, the current 24-hour register input shall be transferred to the recent register. Before the data is transferred, the data in the recent register shall be discarded.

Recent register time stamp: The recent register shall contain a time-stamp indicating the end of the recent interval.

Report recent register: It shall be possible to report the value of the recent registers when requested.

10.2.16 Transient condition threshold function – ThrF-tr

Symbol:

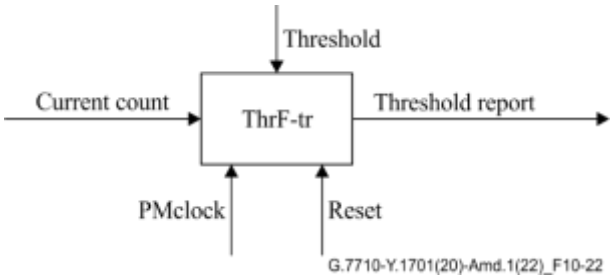


Figure ~~54~~ 10-22 – ThrF-tr

Interfaces:

Table ~~43~~ 10-18 – ThrF-tr input and output signals

Input(s)	Output(s)
Current count Threshold Reset PMclock	Threshold report

Processes:

The transient condition threshold function is used to generate an autonomous threshold report (TR) when the performance of a transport entity falls outside a predetermined level. This function is applicable for 15-minute and 24-hour intervals (refer to clause 10.1.7.2).

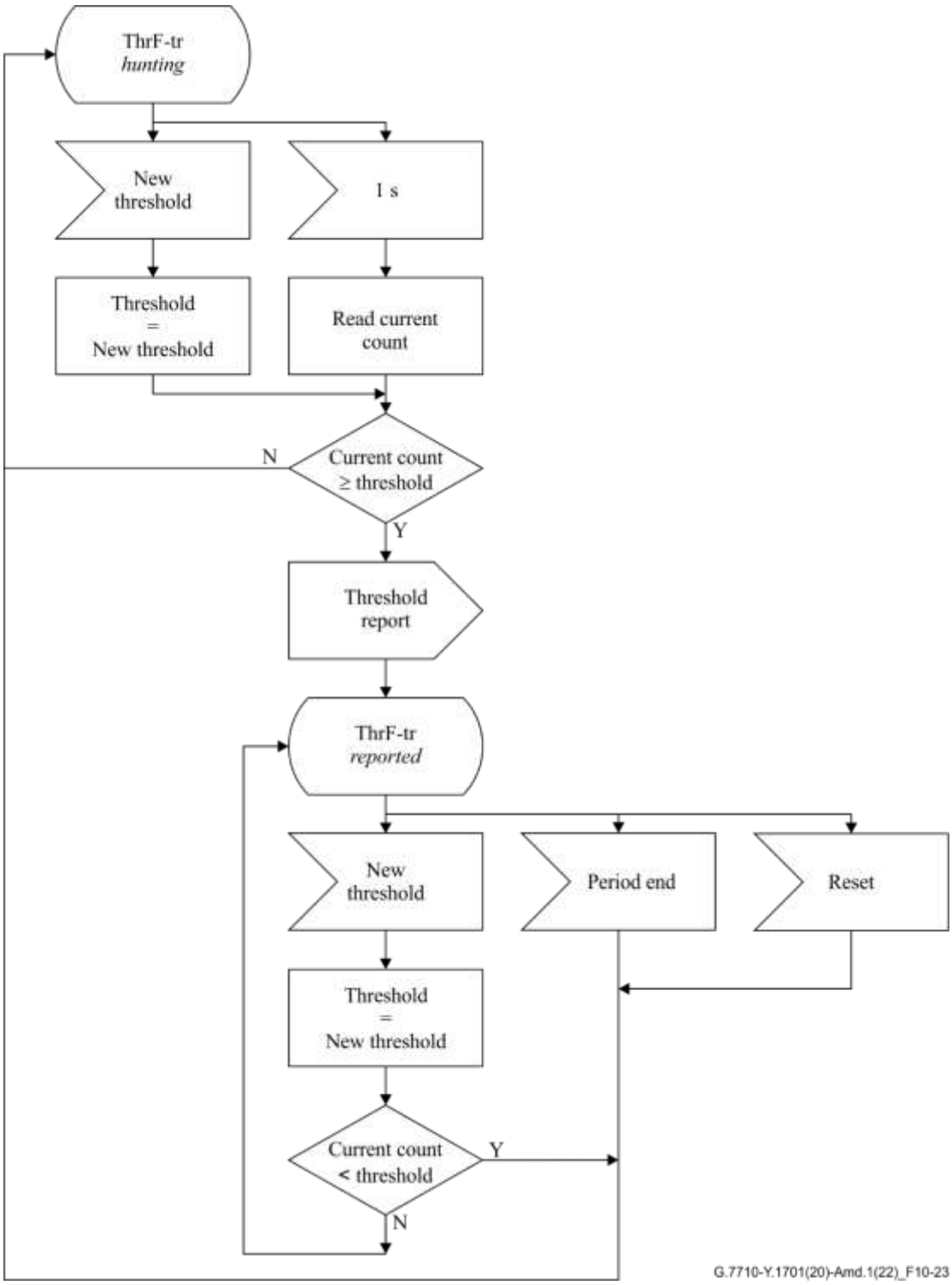


Figure ~~55~~ 10-23 – Transient condition threshold function

The transient condition threshold function shall operate as specified in Figure ~~55~~10-23. Every second, the current count shall be compared with the threshold. A threshold report (TR) shall be sent when the current count is equal to, or larger than, the threshold. When the current count is reset to zero, a TR shall be sent again in the current interval if the count reaches or exceeds the threshold. When the threshold is modified to a value lower than the current count, another TR shall be sent immediately.

A threshold can be crossed at any second within the current interval. The function shall detect a 15-minute threshold crossing within 1 minute of its occurrence, and a 24-hour threshold crossing within 15 minutes of its occurrence. The 15-minute threshold report shall indicate the PM-second of

the occurrence. The 24-hour threshold report shall indicate the moment of threshold crossing detection (that might be up to 15 minutes after the occurrence). The time-stamp shall have a resolution of 1 second.

10.2.17 Standing condition threshold function – ThrF-st

Symbol:

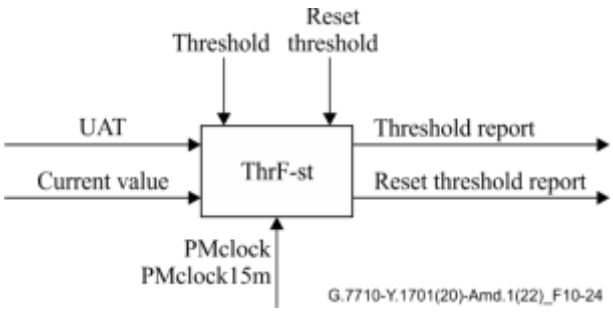


Figure ~~56~~ 10-24 – ThrF-st

Interfaces:

Table ~~44~~ 10-19 – ThrF-st input and output signals

Input(s)	Output(s)
Current value UAT Threshold Reset threshold PMclock PMclock15m	Threshold report Reset threshold report

Processes:

The standing condition threshold function is an option for 15-minute periods. The standing condition is raised, and a TR is generated when the threshold is reached or crossed. The standing condition is cleared, and a reset threshold report (RTR) is generated when, at the end of the period, the current count is below, or equal to, the reset threshold, provided that there was no unavailable time during that period (refer to clause 10.1.7.2).

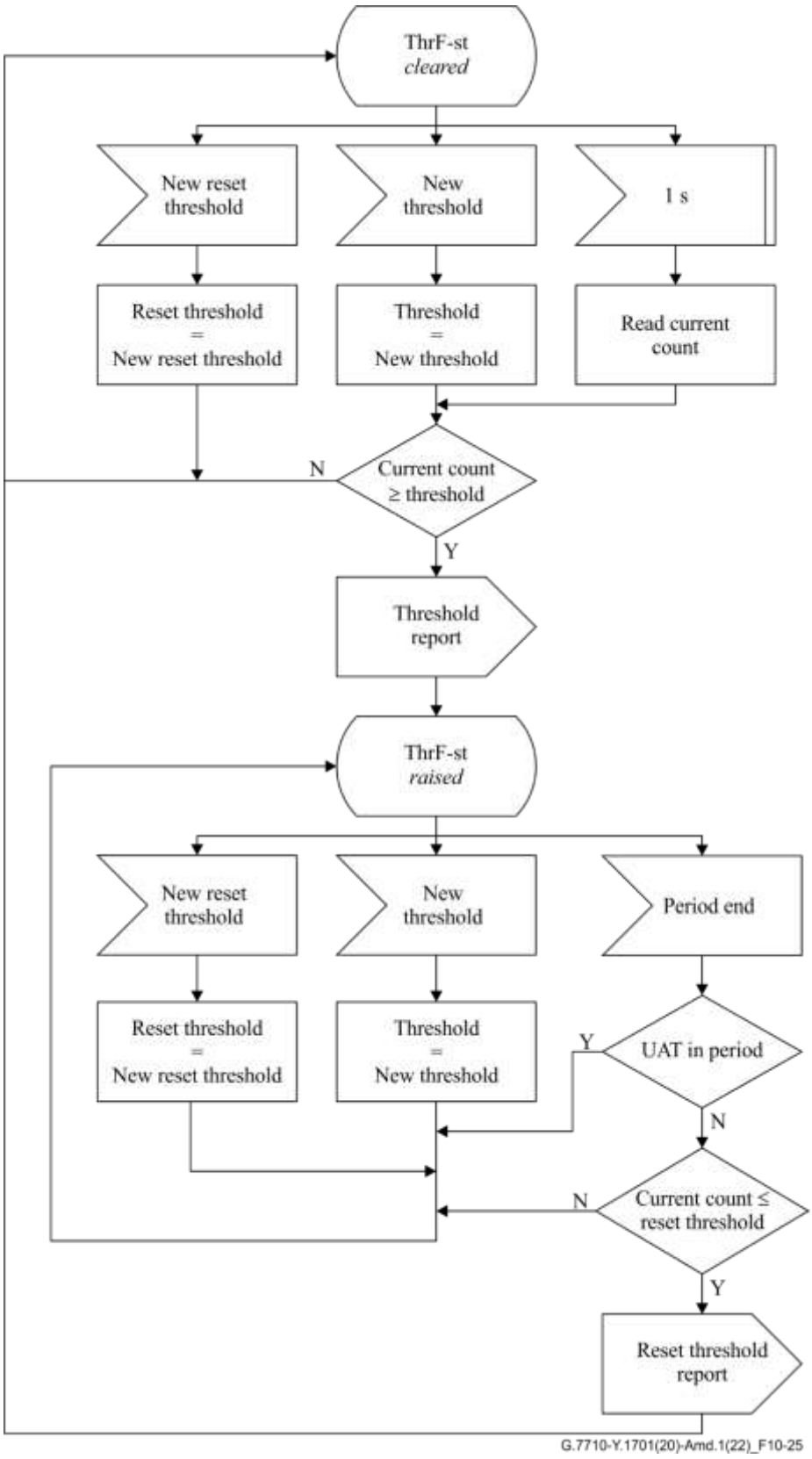


Figure ~~57~~ 10-25 – Standing condition threshold function

The standing condition threshold function shall operate as specified in Figure ~~57~~10-25. When the standing condition is cleared, it shall be set to raised if the (changed) current counter value is equal to, or larger than, the (changed) threshold value. When the standing condition is raised, it shall be set to cleared at the end of a (following) 15-minute period if the current counter value is equal to, or

lower than, the reset threshold value, provided that there is no unavailable time in the period. A threshold report (TR) shall be generated when the standing condition changes from cleared to raised. A reset threshold report (RTR) shall be generated when the standing condition changes from raised to cleared.

NOTE – The behaviour on a change of the threshold value is compliant with [ITU-T M.2120], but not compliant with [ITU-T Q.822]. The latter requires generating an RTR when the threshold is modified to a value larger than the current register value.

A set threshold can be crossed at any second within the current interval. The function shall detect a 15-minute threshold crossing within 1 minute of its occurrence. The 15-minute TR and RTR shall indicate the PM-second of the occurrence. The time-stamp shall have a resolution of 1 second.

10.2.18 Out of range function for gauge overflow detection – ORF-o

Symbol:

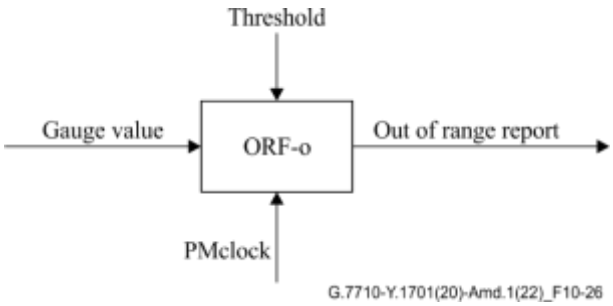


Figure ~~58~~ 10-26 – ORF-o

Interfaces:

Table ~~45~~ 10-20 – ORF-o input and output signals

Input(s)	Output(s)
Gauge value Threshold PMclock	Out of range report

Processes:

The out of range function for gauge overflow detection is used to generate an autonomous out of range report (ORR) when the gauge value of a snapshot or high tidemark is at, or above, a predetermined level. This function is applicable for 15-minute and 24-hour intervals.

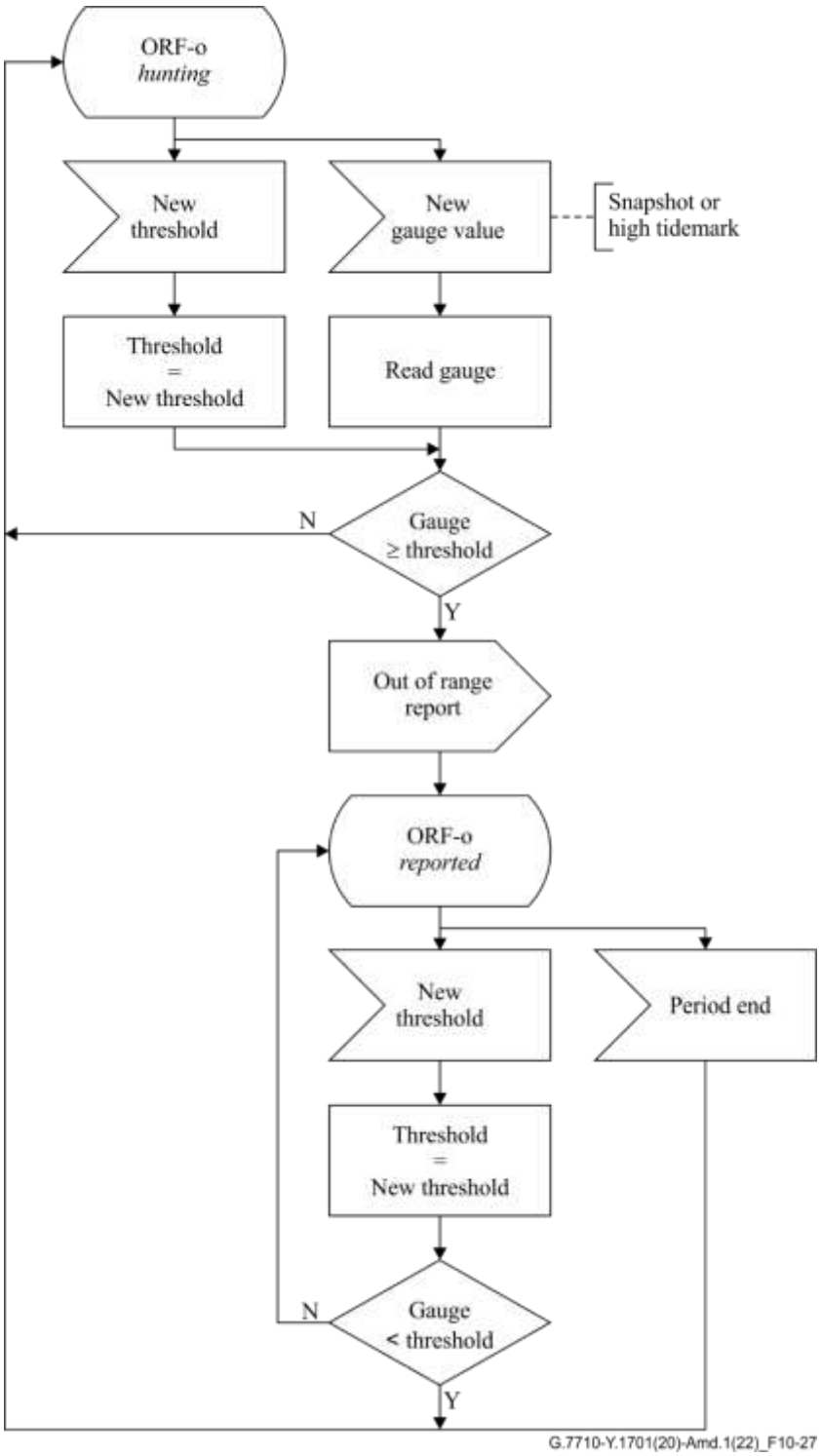


Figure ~~59~~ 10-27 – Out of range function for gauge overflow detection

The out of range function for gauge overflow detection shall operate as specified in Figure ~~59~~10-27. Every time a new gauge value (snapshot or high tidemark) becomes available, the gauge value shall be compared with the threshold. An out of range report (ORR) shall be sent when the gauge is equal to or larger than the threshold. When the threshold is modified to a value lower than the current gauge value, another ORR shall be sent immediately. An ORR shall be sent again when, after resetting, the gauge becomes at or above the new threshold.

A threshold can be crossed at any time within the current interval. The function shall detect a 15-minute threshold crossing within 1 minute of its occurrence, and a 24-hour threshold crossing within 15 minutes of its occurrence. The 15-minute and 24-hour ORR shall indicate the PM-second of the occurrence. The time-stamp shall have a resolution of 1 second.

10.2.19 Out of range function for underflow detection – ORF-u

Symbol:

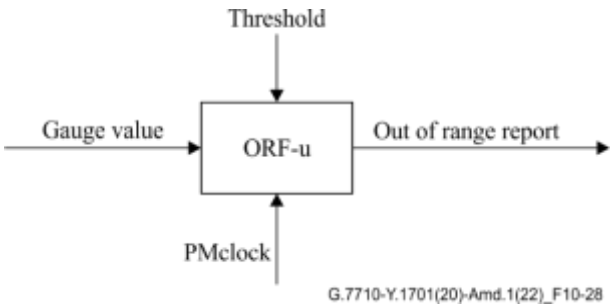


Figure ~~60~~ 10-28 – ORF-u

Interfaces:

Table ~~46~~ 10-21 – ORF-u input and output signals

Input(s)	Output(s)
Gauge value Threshold PMclock	Out of range report

Processes:

The out of range function for gauge underflow detection is used to generate an autonomous out of range report (ORR) when the gauge value of a snapshot or low tidemark is at, or below, a predetermined level. This function is applicable for 15-minute and 24-hour intervals.

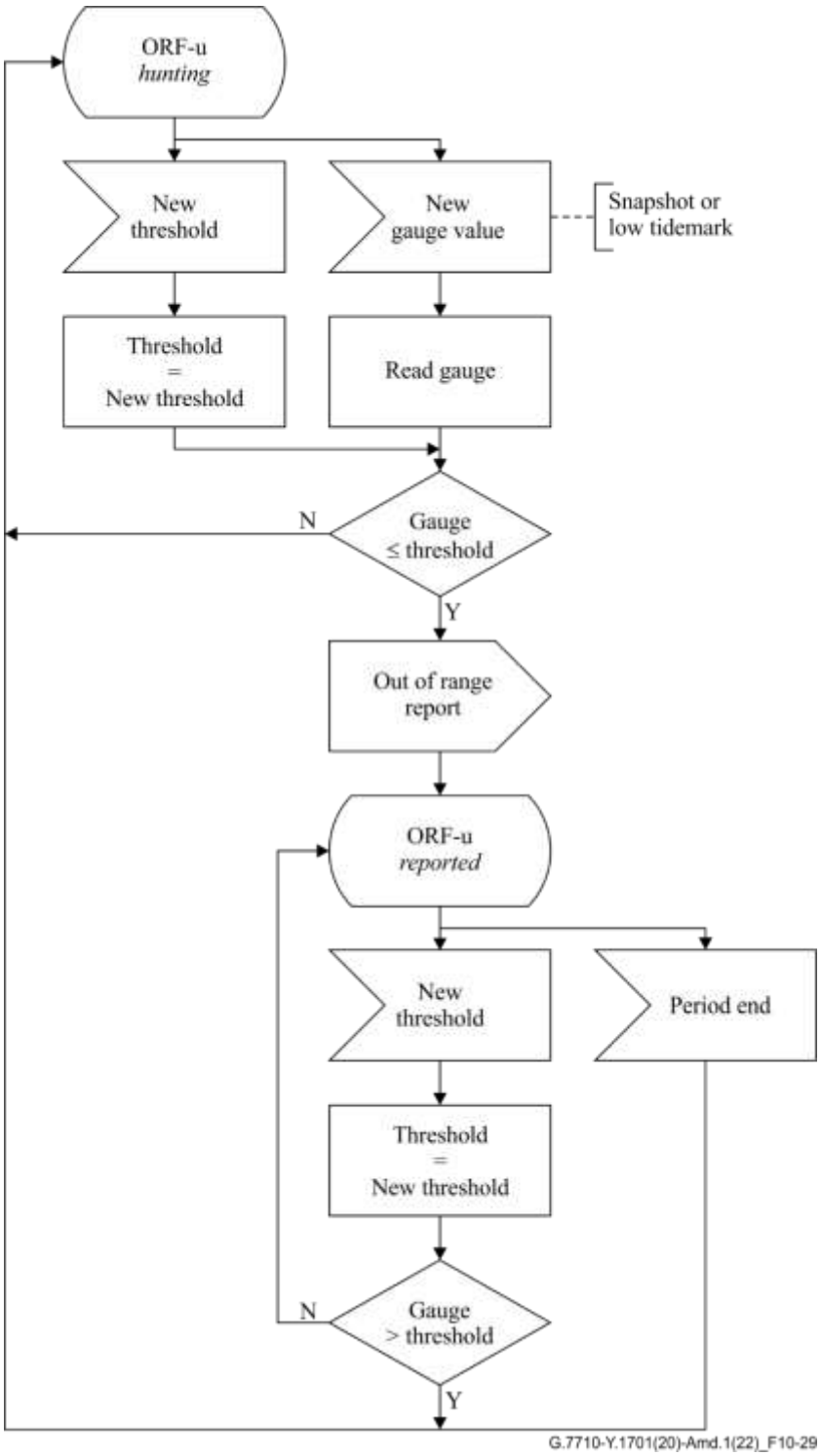


Figure ~~61~~ 10-29 – Out of range function for gauge underflow detection

The out of range function for gauge underflow detection shall operate as specified in Figure ~~61~~10-29. Every time a new gauge value (snapshot or low tidemark) becomes available, the gauge value shall be compared with the threshold. An out of range report (ORR) shall be sent when the gauge is equal to, or smaller, than the threshold. When the threshold is modified to a value higher than the current gauge value, another ORR shall be sent immediately. An ORR shall be sent again, after resetting, the gauge becomes at or below the new threshold.

A threshold can be crossed at any time within the current interval. The function shall detect a 15-minute threshold crossing within 1 minute of its occurrence, and a 24-hour threshold crossing within 15 minutes of its occurrence. The 15-minute and 24-hour ORR shall indicate the PM-second of the occurrence. The timestamp shall have a resolution of 1 second.

11 Security management

See security requirements in [ITU-T M.3016.x].

12 Control plane management

The clause describes the requirements for managing the control functions that are resided in the network element.

12.1 Fault reporting management

Fault reporting management (FRM) provides a function to notify the management/control system about the fault events of the transport element. A typical use case of FRM is the controller-based restoration that is one of the connection availability enhancement techniques in G.7702 for transport networks controlled by SDN controllers. It requires that transport equipment notifies fault events to the SDN controller immediately when the fault events occur in order to minimize interrupted service time. The FRM function processes fault events received from the transport plane atomic functions and report them to the SDN controller. It has internal functions that network operators can program their own types of fault events used to trigger the controller-based restoration. Figure ~~62~~12-1 is a functional model of the FRM that consists of three functional blocks: fault event registration, fault event filtering, and fault event reporting.

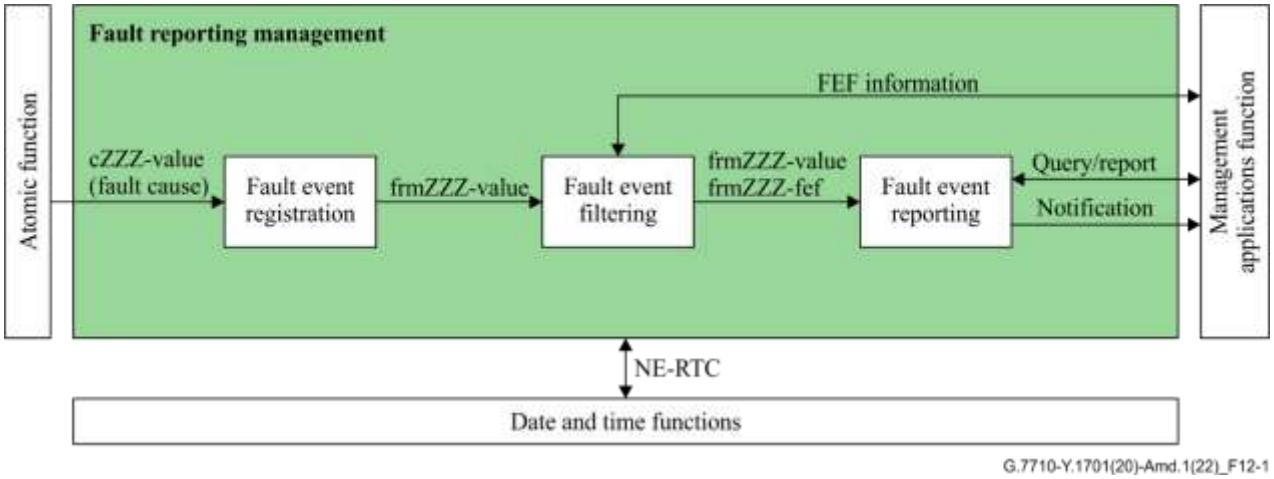


Figure ~~62~~12-1 – FRM functional diagram

12.1.1 Fault event registration

The fault event registration function receives a fault event from the Atomic function, extracts information of the FRM fault required to trigger the controller-based restoration based on the incoming fault event and registers it with arrival timestamp.

The fault event registration function is responsible for integration of fault causes MI_cZZZ into FRM fault frmZZZ-value that includes identification of the managed entity and its location, an indication whether the fault has been raised or cleared, and a timestamp of this event.

The FRM fault event declaration and clearing shall be time-stamped. For declaration, the timestamp shall indicate the time at which the fault cause is activated at the input of the fault event registration

block. For clearing, the time-stamp shall indicate the time at which the fault cause is deactivated at the input of the fault event registration block.

12.1.2 Fault event filtering

Depending on the FRM configuration information received from the SDN controller, the fault event filtering (FEF) function decides whether incoming fault events shall be reported or not for the controller-based restoration.

The FEF function is responsible for assigning a value to the frmZZZ-fef variable. The assignment shall be possible per managed entity and is based on the "FEF information". The "FEF information" sent from the SDN controller is used for classification to decide on which faults shall be reported for the controller-based restoration.

The frmZZZ-fef value shall be "reported" when the "FEF information" specifies the probable cause to be "reported". The frmZZZ-fef value shall be "not reported" when the "FEF information" specifies the probable cause to be "not reported". The fault value accompanied with the assigned frmZZZ-fef shall become available at the output of the FEF function.

Note that the FEF information includes the fault list that has been requested to be reported per managed entity.

12.1.3 Fault event reporting

The fault event reporting function notifies to the SDN controller only the fault events identified as the reportable fault. It also stores all reportable fault events in order to synchronize the SDN controller. Upon query, the stored fault information shall be reported.

Appendix I

Overview of common and technology-specific ITU-T Recommendations

(This appendix does not form an integral part of this Recommendation.)

Figure I.1 – Common and technology-specific ITU-T Recommendations

Appendix II

Protocol to set the local real-time clock within a few seconds relative to the external time reference

(This appendix does not form an integral part of this Recommendation.)

This mechanism assumes that the time for a message to be sent from the element management system (EMS) to the network element (NE) is not significantly different from that of the time it takes for the reply to return from the NE to the EMS.

The mechanism also assumes that the message round trip time is meaningful in that the processing time within the NE is negligible, so a simple message that gets a small response shall be used.

II.1 Measure round trip time

The round trip time, *t*, between sending a message and receiving the reply ($T_2 – T_1$ in Figure II.1) is calculated a number of times. The mean and maximum difference (maximum time minus minimum time) for the round trip time is determined. The messages that are used to determine the round trip time are also used to request the NE's internal time (T_{NE} in Figure II.1), which is returned in the replies to the EMS.

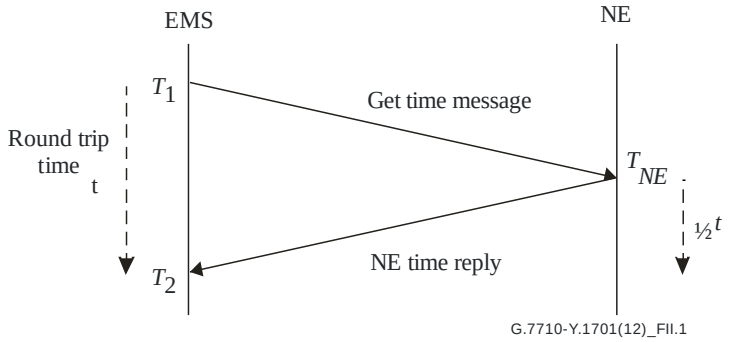


Figure II.1 – Round trip time

The mean round trip time is used to validate whether the traffic on the network is low, i.e., there are currently no significant delays being experienced by a message being sent to this NE. The maximum difference in message round trip times is used as a measure of the stability of the path between the EMS and NE across the network, i.e., constant and not varying due to fluctuations of traffic on the network.

If the mean and maximum are within the required boundaries, the time drift between the EMS and NE clocks is calculated.

II.2 Calculate the time drift

The time drift is the difference in time between the EMS clock and the NE clock. The time drift is calculated with the formula:

$$\text{time drift} = T_2 – (T_{NE} + ½\ t)$$

which can easily be validated from Figure II.1 above. When the time drift exceeds the synchronization requirement, the NE clock needs to be set.

II.3 Set NE clock

To set the NE clock, the EMS sends the set time message containing the momentary EMS time (T_3 in Figure II.2) plus an offset. This offset is equal to half the mean value of the round trip time.

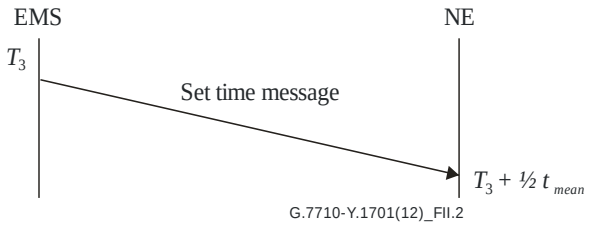


Figure II.2 – Set NE clock

Upon receipt of the set time message, the NE sets its clock to the time indicated in the message.

Appendix III

SDH and PDH Implementations of termination point mode and port mode

(This appendix does not form an integral part of this Recommendation.)

It must be noted that for SDH and PDH implementations there are several ways to suppress alarms (see Figure III.1). The trail termination point mode (TPmode) and port mode (Portmode), entering the defect correlation function, can be set to "Not Monitored" (NMON) to suppress the fault cause. The ZZZ_Reported indication, entering the defect correlation function, can be set to "Not Reported" to suppress the fault cause. These mechanisms, outlined in Figure 7-6 stop the information flow at the suppression point. Consequently, the alarm information does not become available at the management interface.

NOTE – For new implementations (e.g., OTN equipment), this method has been replaced by the ARC method, defined in clause 7.2.3, because it can cause maintenance problems.

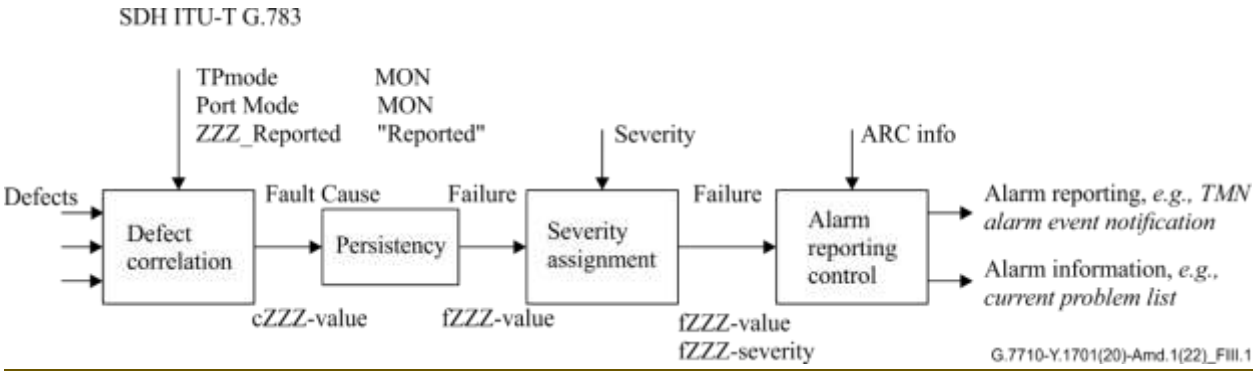


Figure III.1 – Report options in combination with previous alarm suppressing mechanisms

For implementations supporting both the ARC and previous alarm suppression mechanisms, it is required to have specific values for the previous mechanisms in order to allow the ARC function to control the alarm reporting and information facilities. The specific value for the trail termination point mode and the port mode is "monitored" (MON), the specific value for ZZZ_Reported is "Reported".

Appendix IV

Administrative state examples

(This appendix does not form an integral part of this Recommendation.)

This appendix provides examples of applying the administrative states on a server layer trail and tandem connection monitoring (TCM).

IV.1 Lock a server layer trail

Figure IV.1 shows a dual-sided locking of a server layer trail where the administrative locking is applied to the adaptation function at both edges of the server layer trail. The administrative locking is applied to the whole adaption functions. The requirements and behaviour of administrative locking described in clause 8.15 apply to both the source and sink directions of the adaptation function, as shown by the solid and dash lines of Client LCK signal flows in the figure.

Single-sided locking of a server layer trail is also possible when the administrative locking is applied to the adaptation function only at one edge of the server layer trail.

When the server layer trail is administrative locked, server layer path monitoring is still working. This allows the operator to validate that the server layer path is operational before unlocking the trail.

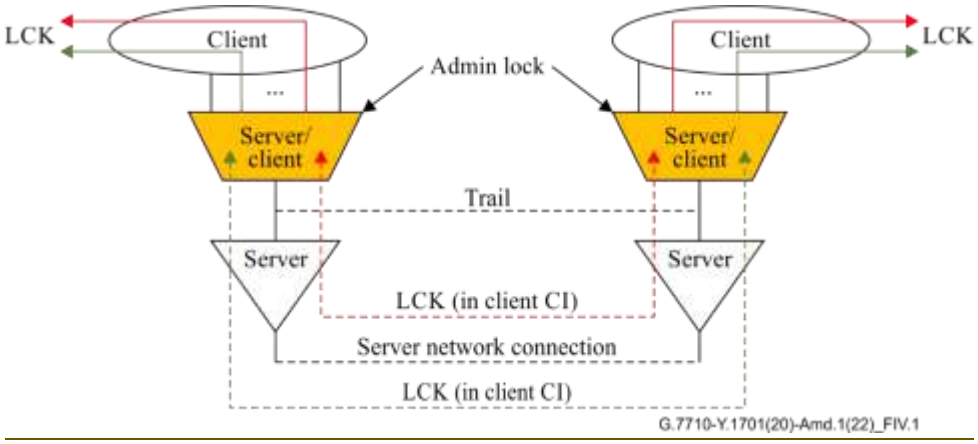


Figure IV.1 – Locking a server layer trail

IV.2 Lock a tandem connection

Figure IV.2 shows a dual-sided locking of a tandem connection where the administrative locking is applied to the adaptation function at both edges of the tandem connection. The administrative locking is applied to the whole adaption functions. The requirements and behaviour of administrative locking described in clause 8.15 apply to both the source and sink directions of the adaptation function, as shown by the solid and dash lines of Client LCK signal flows in the figure.

Single-sided locking of a tandem connection is also possible when the administrative locking is applied to the adaptation function only at one edge of the tandem connection.

When the tandem connection is administrative locked, TCM is still working. This allows the operator to validate that the tandem connection is operational before unlocking it.

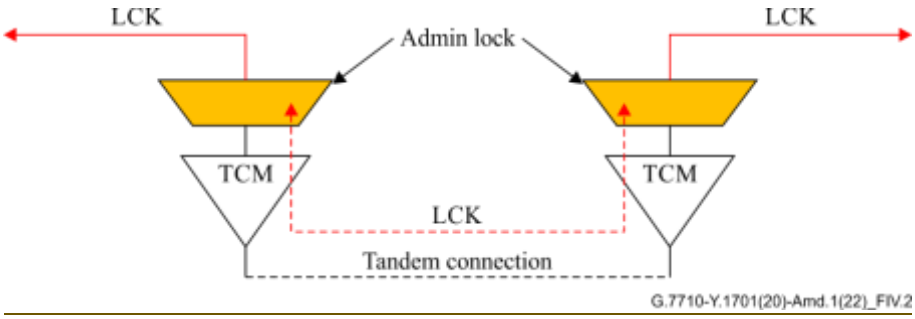


Figure IV.2 – Locking a tandem connection

Bibliography

[b-ITU-T G.783] Recommendation ITU-T G.783 (2006), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.*

[b-ITU-T G.784] Recommendation ITU-T G.784 (2008), *Management aspects of synchronous digital hierarchy (SDH) transport network elements.*

[b-ITU-T G.798] Recommendation ITU-T G.798 (2017), *Characteristics of optical transport network hierarchy equipment functional blocks.*

[b-ITU-T G.803] Recommendation ITU-T G.803 (2000), *Architecture of transport networks based on the synchronous digital hierarchy (SDH).*

[b-ITU-T G.872] Recommendation ITU-T G.872 (2017), *Architecture of optical transport networks.*

[b-ITU-T G.874] Recommendation ITU-T G.874 (2017), *Management aspects of optical transport network elements.*

[b-ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks.*

[b-ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2018), *Characteristics of Ethernet transport network equipment functional blocks.*

[b-ITU-T G.8051] Recommendation ITU-T G.8051/Y.1345 (2018), *Management aspects of the Ethernet-over-Transport (EoT) capable network element.*

[b-ITU-T G.8110.1] Recommendation ITU-T .8110.1/Y.1370.1 (2011), *Architecture of the Multi-Protocol Label Switching transport profile layer network.*

[b-ITU-T G.8121.x] Recommendation ITU-T G.8121/Y.1381 series:

Recommendation ITU-T G.8121/Y.1381 (2018), *Characteristics of Transport MPLS equipment functional blocks.*

Recommendation ITU-T G.8121.1/Y.1381.1 (2018), *Characteristics of MPLS-TP equipment functional blocks supporting ITU-T G.8113.1/Y.1372.1 OAM mechanisms.*

Recommendation ITU-T G.8121.2/Y.1381.2 (2018), *Characteristics of MPLS-TP equipment functional blocks supporting ITU-T G.8113.2/Y.1372.2 OAM mechanisms.*

[b-ITU-T G.8151] Recommendation ITU-T G.8151/Y.1374 (2018), *Management aspects of the T-MPLS network element.*

[b-ITU-T I.326] Recommendation ITU-T I.326 (2003), *Functional architecture of transport networks based on ATM.*

[b-ITU-T I.732] Recommendation ITU-T I.732 (2000), *Functional characteristics of ATM equipment.*

[b-ITU-T I.751] Recommendation ITU-T I.751 (1996), *Asynchronous transfer mode management of the network element view.*

[b-ANSI T1.231] ANSI Standard T1.231 (1997), *Digital Hierarchy – Layer 1 In-Service Digital Transmission Performance Monitoring*.

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	**Y.1700–Y.1799**
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
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, and associated measurements and tests
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, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023