

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.7710/Y.1701

Amendment 1
(11/2016)

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

Recommendation ITU-T G.7710/Y.1701 (2012) –
Amendment 1



Documents
Document Sharing Hub

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 2012 revision of this Recommendation has incorporated the following below.

- Recommendation ITU-T G.7710/Y.1701 Corrigendum 1 (11/2009):
this mainly contains an updated equipment management function process block diagram.
- Recommendation ITU-T G.7710/Y.1701 Amendment 1 (07/2010):
updates the packet layer related specification of severely errored second (SES) to align it with the SES definition in Recommendation ITU-T Y.1563.
- Recommendation ITU-T G.7710/Y.1701 Corrigendum 2 (04/2011):
this adds the missing 6 LBC terms to the process description, and
- gives additional specifications on gauge measurement.

Amendment 1 provides updates to:

- Clause 3.2.2 definition of the term Local Craft Terminal
- Clause 6.1.5 "Management of the DCN"
- Clause 8.9.1 "Provisioning" Table 21 "Alarm severity provisioning"
- Clause 8.14 for optical power monitoring and control

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

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 not received notice of intellectual property, protected by patents, 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 TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	3
	3.1 Terms defined elsewhere	3
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	4
5	Conventions	9
6	Management architecture.....	9
	6.1 Network management architecture.....	10
	6.2 Equipment management architecture	15
7	Fault management.....	17
	7.1 Fault management applications	17
	7.2 Fault management functions.....	23
8	Configuration management	32
	8.1 Hardware	33
	8.2 Software.....	33
	8.3 Protection switching	34
	8.4 Trail termination.....	34
	8.5 Adaptation	36
	8.6 Connection.....	36
	8.7 DEG thresholds	40
	8.8 XXX_Reported.....	40
	8.9 Alarm severity	40
	8.10 Alarm reporting control (ARC).....	41
	8.11 PM thresholds.....	41
	8.12 Tandem connection monitoring (TCM) activation.....	41
	8.13 Date and time.....	42
	8.14 Optical power monitoring and control	47
9	Account management	47
10	Performance management	48
	10.1 Performance management applications.....	48
	10.2 Performance monitoring functions	59
11	Security management.....	86
	Appendix I – Overview of common and technology-specific ITU-T Recommendations.....	87
	Appendix II – Protocol to set the local real-time clock within a few seconds relative to the external time reference	88

	Page
II.1 Measure round trip time	88
II.2 Calculate the time drift	88
II.3 Set NE clock	89
Bibliography.....	90

Copyright © 2016 by ITU-T

Recommendation ITU-T G.7710/Y.1701

Common equipment management function requirements

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 (2012).

1 Scope

This Recommendation specifies those equipment management function (EMF) requirements that are common to multiple transport technologies. 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.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.
- [ITU-T G.806] Recommendation ITU-T G.806 (2009), *Characteristics of transport equipment – Description methodology and generic functionality*.
- [ITU-T G.808.1] Recommendation ITU-T G.808.1 (2010), *Generic protection switching – Linear trail and subnetwork protection*.
- [ITU-T G.809] Recommendation ITU-T G.809 (2003), *Functional architecture of connectionless layer networks*.
- [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.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
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
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
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
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
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
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
WS	Work Station
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 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 work station (WS) attached to the OSF.

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

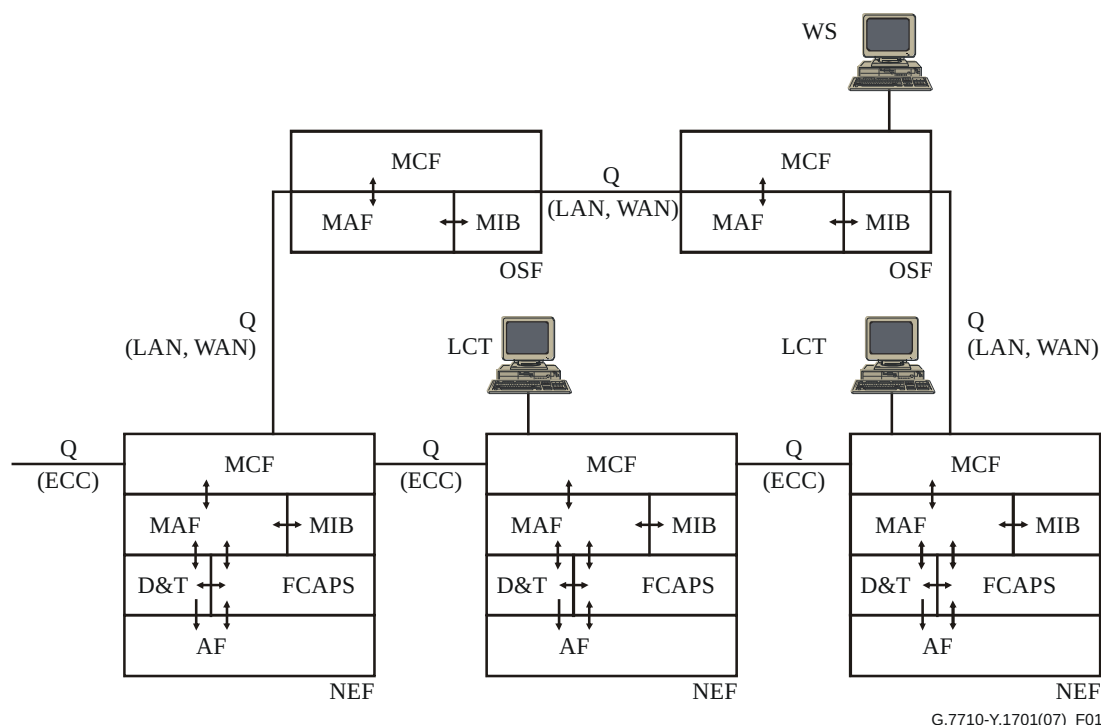


Figure 1 – Management organizational model

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 1, are not within the scope of this Recommendation.

6.1 Network management 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 2 for an optical management network, an SDH management network, and another (x) management network.

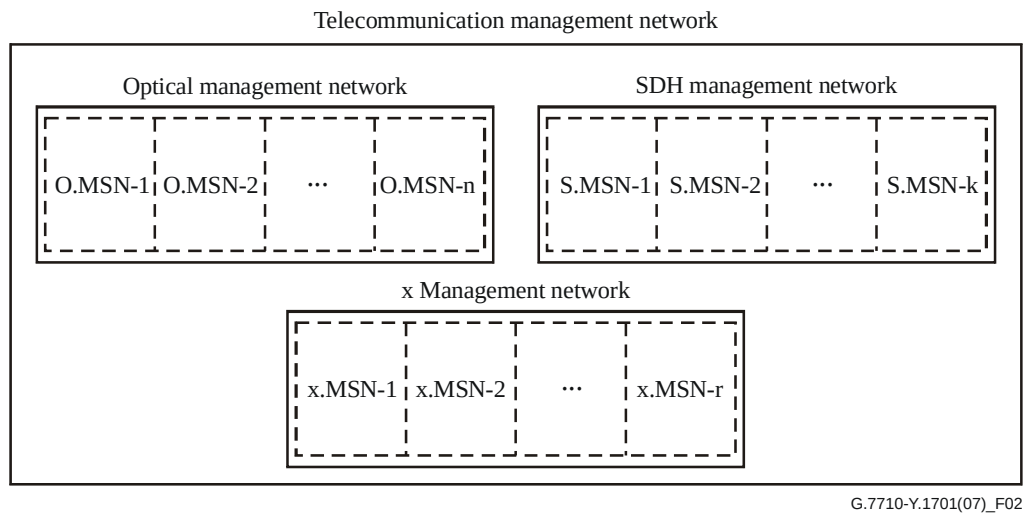
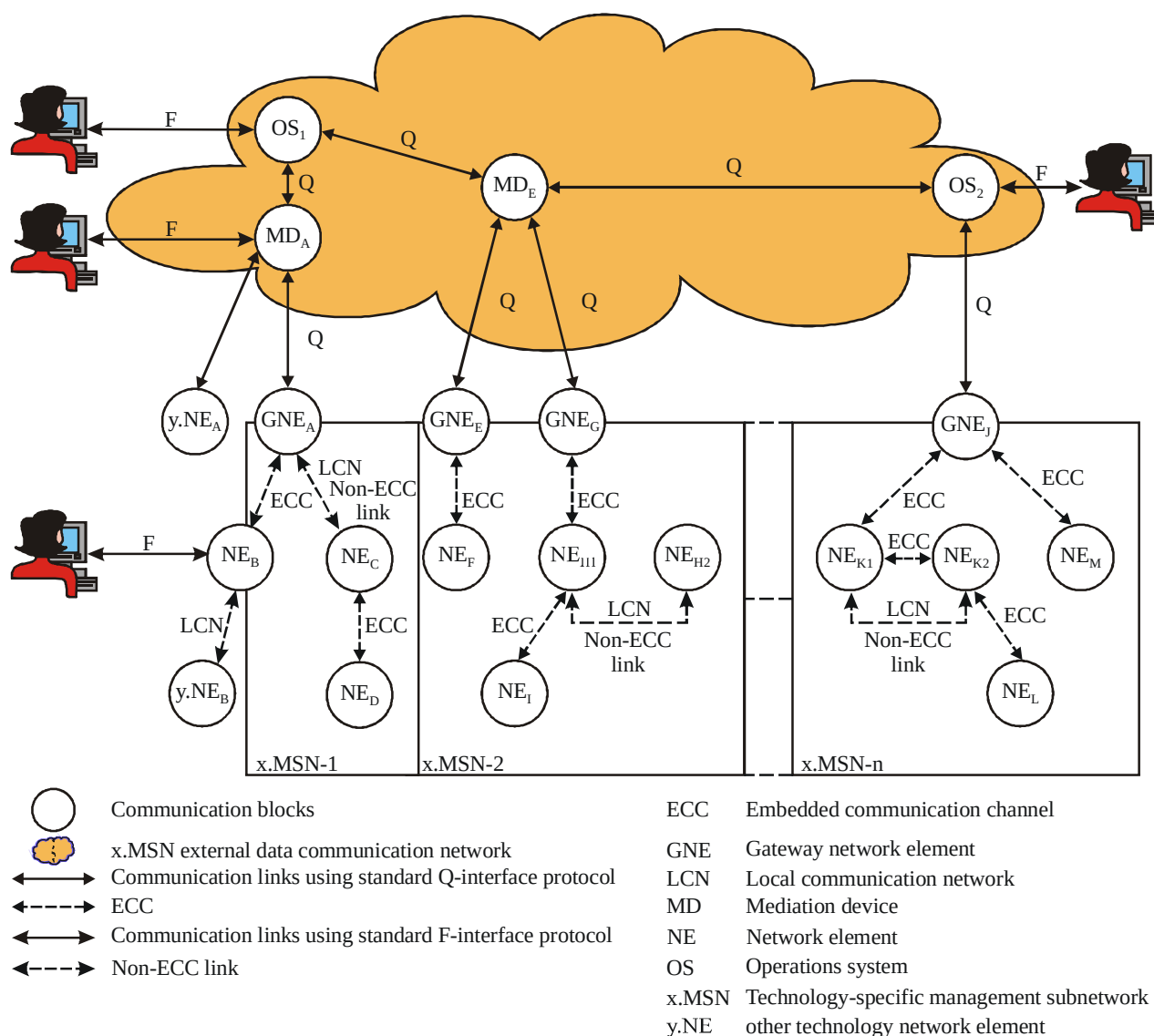


Figure 2 – TMN, x.MN and x.MSN partitioning

Figure 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].



G.7710-Y.1701(07)_F03

Figure 3 – Management network example**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 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 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.

d) *Intra-site communications*

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

NOTE – A standardized LAN for communicating between collocated network elements has been proposed as an alternative to the use of an ECC. The LAN would potentially be used as a general site communications network serving all NEs. The specification of the LAN is beyond the scope of this Recommendation and is defined in [ITU-T G.7712].

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 3. The GNE should be able to perform an intermediate system network layer routing function for ECC 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.

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. ~~Examples are:~~

- 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 4 shows such a client-server relationship between two different management subnetworks.

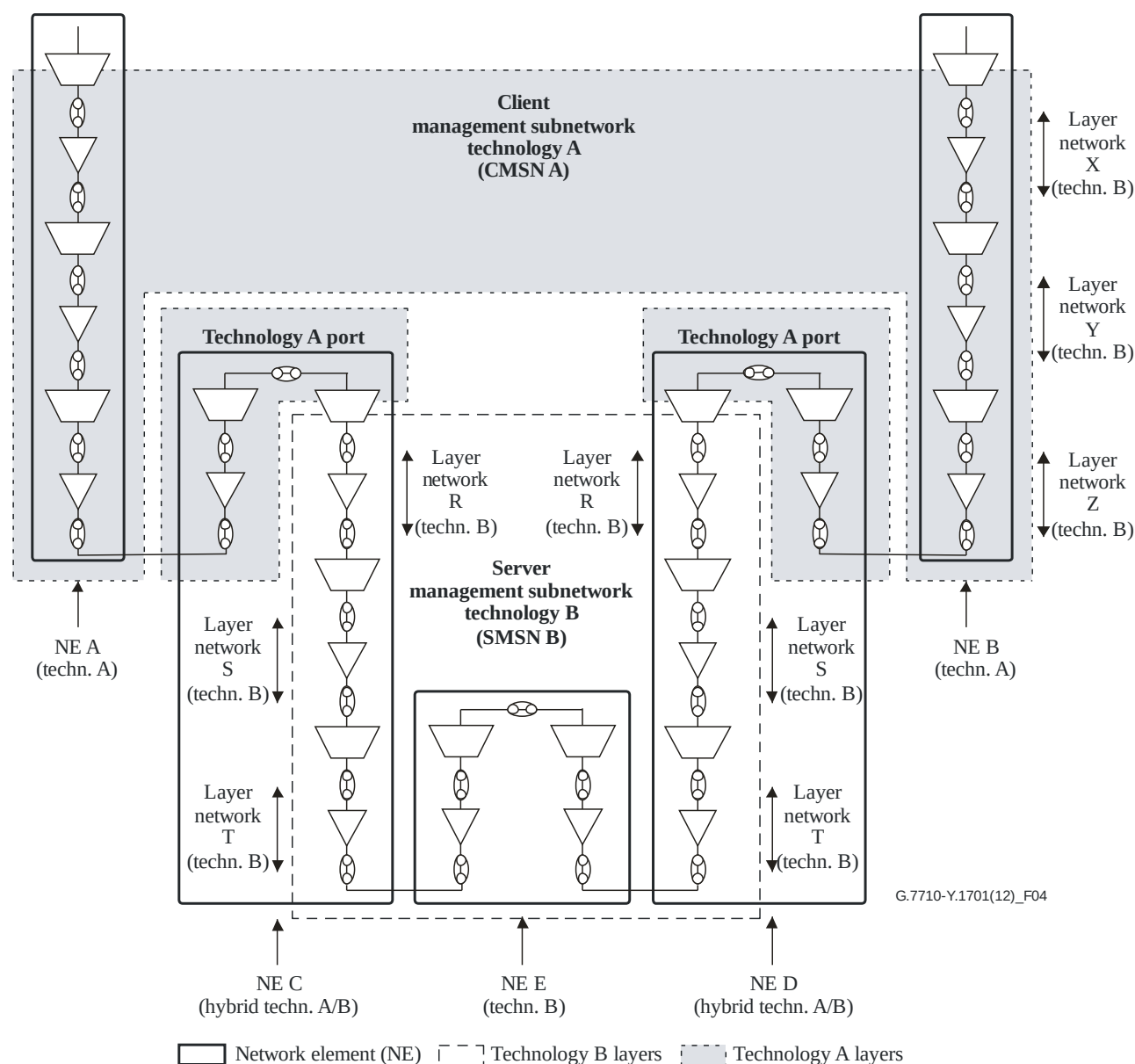


Figure 4 – Example of management network relationships

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 SMSN) for each domain, which may or may not be collocated in the same physical OS.

6.2 Equipment management architecture

The equipment management function (EMF) provides the means through which an element management system (EMS) and other managing entities manage the network element function (NEF). Figure 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).

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 provides event message processing, data storage and logging. 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.

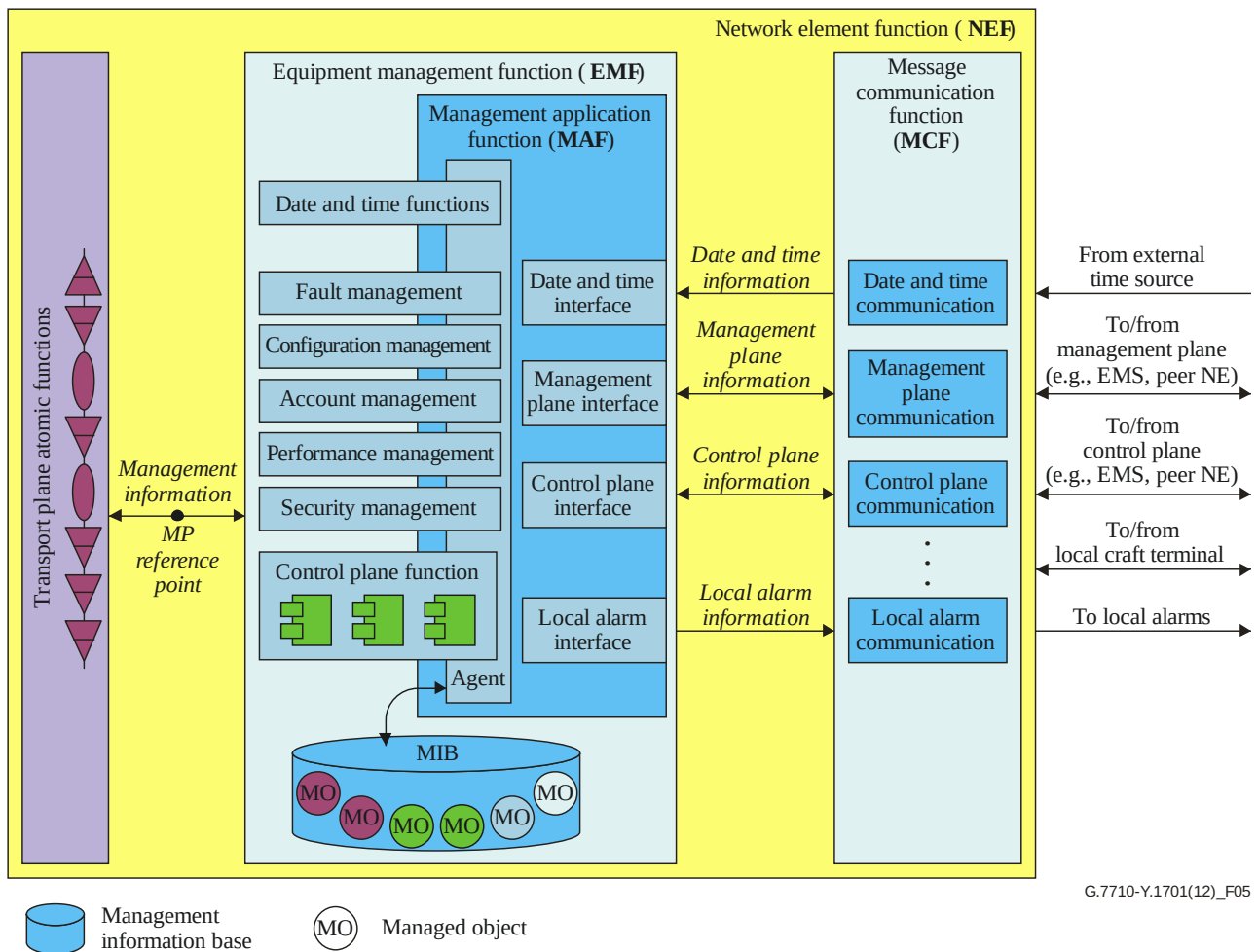


Figure 5 – Equipment management function process block diagram

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.

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.

Copyright International Telecommunication Union

– *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.805] (for connection-oriented networks), [ITU-T G.809] (for connectionless 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.

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 1 gives examples.

Table 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).		

Table 1 – Atomic function associated transmission failure list

	Termination sink	Adaptation sink	Connection
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 2 summarizes these categories.

Table 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 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.

Copyright © 2016 ITU-T

7.1.3.2 Alarm reporting control

Alarm reporting control (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 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.

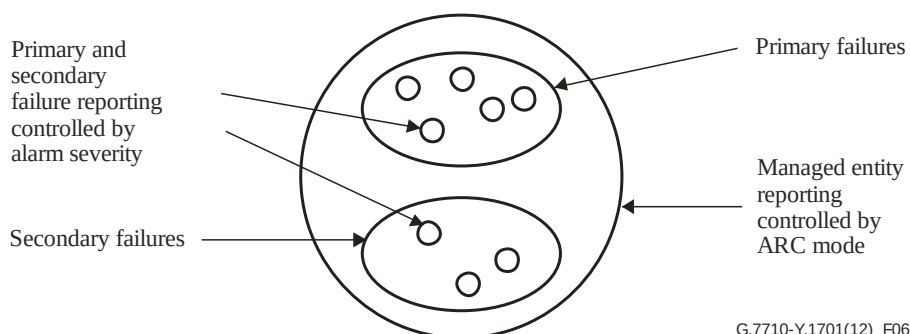


Figure 6 – Managed entity with associated failures

7.1.3.4 Alarm reporting

Alarm reporting is concerned with the 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 the events and conditions that generate autonomous reports and those that shall be reported on request.

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 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.

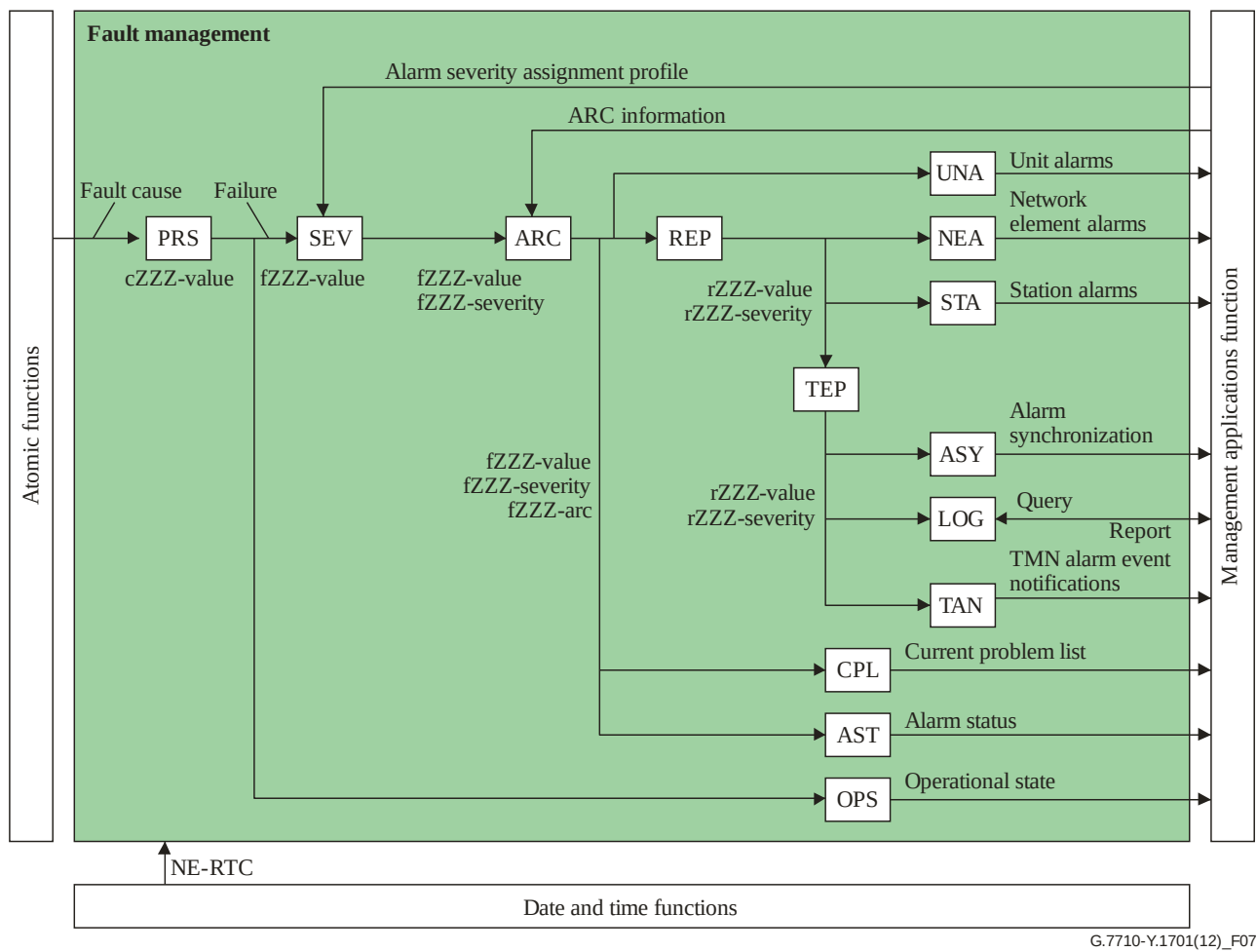


Figure 7 – Fault management inside the EMF

7.2.1 Fault cause persistency function – PRS

Symbol:

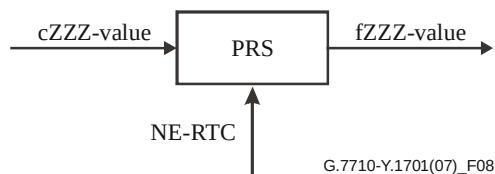


Figure 8 – Fault cause persistency function

Interfaces:

Table 3 – Fault cause persistency input and output signals

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