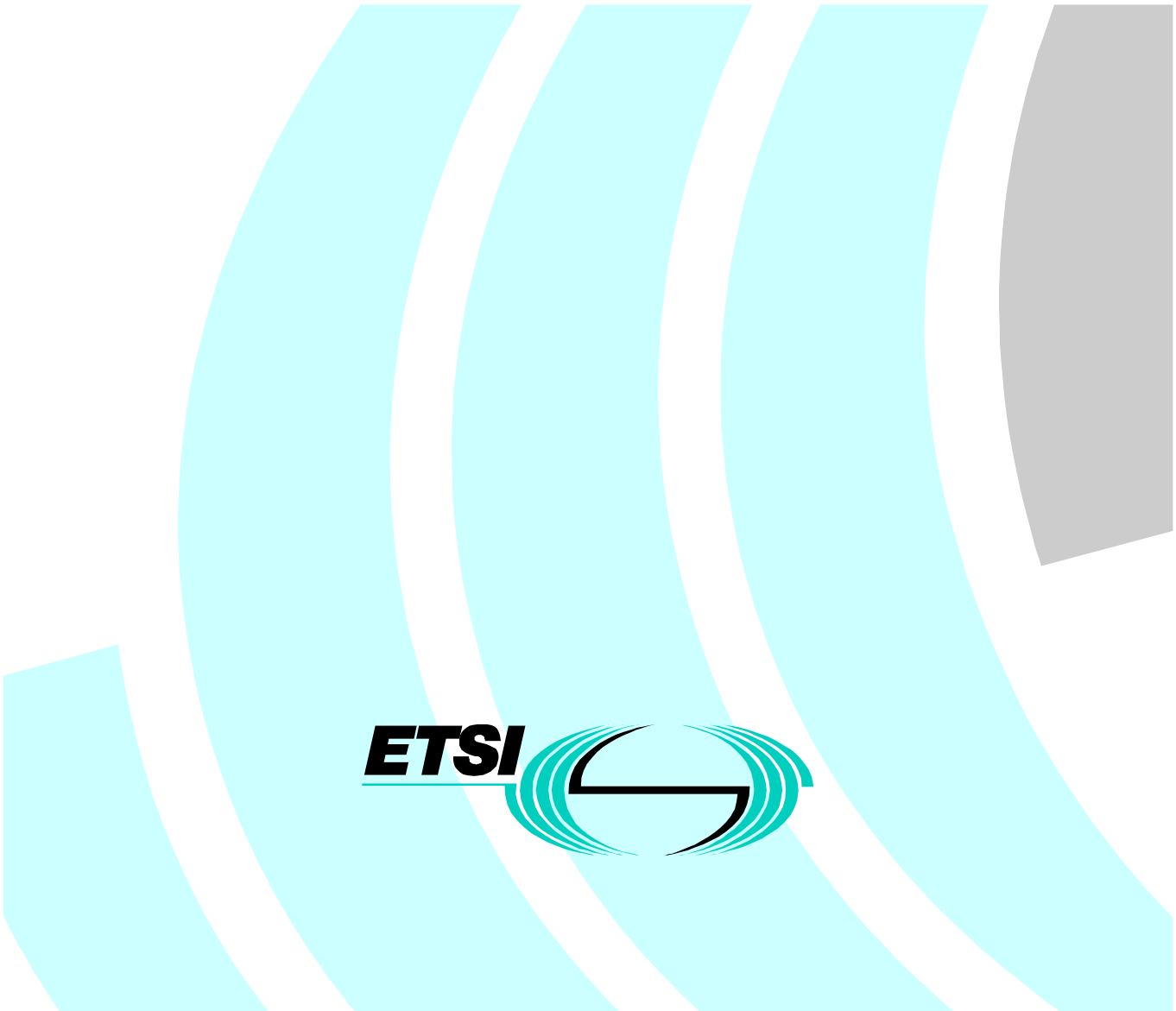
EN 300 820-2 V1.2.3 (1998-07)

European Standard (Telecommunications series)

Telecommunications Management Network (TMN); Management information model for the X-type interface between Operation Systems (OSs) of a Virtual Path (VP)/Virtual Channel (VC) cross connected network; Part 2: Asynchronous Transfer Mode (ATM) VP alarm management



Reference
DEN/TMN-00032 (7lci0iq0.PDF)

Keywords
B-ISDN, broadband, ISDN, management

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Telecommunications Management Network (TMN).

The present document is part 2 of a multi-part EN covering the management information model for the X-type interface between Operation Systems (OSs) of a Virtual Path (VP)/Virtual Channel (VC) cross connected network, as identified below:

Part 1: "Configuration management aspects";

Part 2: "Asynchronous Transfer Mode (ATM) VP alarm management";

Part 3: "Performance management aspects".

National transposition dates	
Date of adoption of this EN:	3 July 1998
Date of latest announcement of this EN (doa):	31 October 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 April 1999
Date of withdrawal of any conflicting National Standard (dow):	30 April 1999

1 Scope

The present document addresses the requirements of network and service providers of Asynchronous Transfer Mode (ATM) cross connected networks for managing the fault alarms associated with the Virtual Path (VP) connections, which span several administrative ATM domains. These requirements are satisfied by the use of a standardized interface (the "X-interface") between Operation Systems (OSs) belonging to different Public Network Operators (PNOs).

The present document describes the X-interface VP alarm management area covering the following aspects:

- the Management Services (MS) and Management Functions (MF) needed that provide the necessary alarm messages for faults detected within ATM Connections which span several administrative domains;
- the management information crossing the X-interface. This management information specification uses the Guidelines for the Definition of Managed Objects (GDMO) formalism, described in ITU-T Recommendation X.722 [2].

The present document has been named as "ATM VP alarm management" because it is expected to be part of a comprehensive fault management standard for ATM VP and Virtual Channels (VCs) in due course. As such it is self-sufficient for the defined scope of reporting faults on, and recovery procedures for, VPs across the X-interface.

2 Normative references

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] EN 300 820-1: "Network Aspects (NA); Management information model for the X-type interface between Operation Systems (OSs) of a Virtual Path (VP)/Virtual Channel (VC) cross connected network; Part 1: Configuration management aspects".

[2] ITU-T Recommendation X.722: "Information Technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects".

[3] ITU-T Recommendation G.805: "Generic functional architecture of transport networks".

[4] ITU-T Recommendation M.3010: "Principles for a Telecommunications Management Network".

[5] ITU-T Recommendation X.721: "Definition of Management Information".

[6] ITU-T Recommendation X.733: "Information Technology - Open Systems Interconnection - Systems management: Alarm reporting function".

[7] ITU-T Recommendation M.3400: "TMN management functions".

[8] ITU-T Recommendation X.734: "Event report management function".

[9] ITU-T Recommendation X.208: "Specification of Abstract Syntax Notation One".

[10] Network Management Forum NMF025: "The 'Ensembles' Concepts and Format", Issue 1.0, August 1992.

[11] ITU-T Recommendation X.711: "Common management information protocol specification for CCITT Applications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

(Some definitions depend on the future acceptance of the "cascaded/mixed mode" as described in EN 300 820-1 [1]. This dependence is already taken into account in these definitions).

access point: It is defined in ITU-T Recommendation G.805 [3].

A Public Network Operator (A PNO): The A PNO is the PNO whose subnet is connected to the A user, the user where the overall VP-connection starts. The A PNO can be the initiating one, but this is not always the case. If it is the initiating PNO it is the root of the X-interface tree. If not, it is the most left leaf (as indicated in figure 1).

If, in future the "cascaded" mode should be accepted as defined in EN 300 820-1 [1], and if the A PNO also acts as initiating PNO, then the A PNO is the consumer of the other PNO's parts of the VP connection.

cascade organization: It is described in EN 300 820-1 [1]. The impact of this organization on the model is for further study.

connection: A "transport entity" which is capable of transferring information transparently between "connection points". A "connection" defines the association between the "connection points" and the "connection points" delimit the "connection".

consumer and provider roles of a PNO: With respect to a particular VP, a PNO acts as a consumer if it has delegated the management of a VP subnetwork connection plus the outgoing link connection (both shall be part of the connection) to another PNO (that acts as a provider). If, in future, the "cascaded/mixed" mode should be accepted (EN 300 820-1 [1]), a PNO can have both roles at once, if it is providing part of the VP (acting as a provider), and at the same time asks another PNO to provide a part of the connection (acting as a consumer).

destination PNO: Z PNO (This term was used in older versions of the specification).

initiating Network Operator (PNO): The initiating PNO is the PNO requesting a particular ATM connection starting in the A subnetwork and ending in the Z subnetwork; it controls the overall VP connection.

Inter PNO Physical Link (IPPL): It represents a physical link that offers bi-directional transmission capabilities and connects two pnoVpSubnetworks. Each InterPNOPhysicalLink is terminated by two pnoNWAtmAccessPoints which are in charge of emitting failures related to the link or to the access point itself. An IPPL can be realized by any transmission capability (SDH, PDH etc.). There is no explicit managed object defined in the X-interface that represents this resource. Information about IPPLs is included in the interPNOTopologicalSubnetworkPair object, EN 300 820-1 [1].

link connection: A "transport entity" provided by the "client/server" association. It is formed by a near-end "adaptation" function, a server "trail" and a far-end "adaptation" function between "connection points". It can be configured as part of the "trail management process" in the associated server layer.

Link: A "topological component" which describes the fixed relationship between a "sub-network" and another "sub-network" or "access group".

mixture organization: It is described in EN 300 820-1 [1]. The impact of this organization on the X-interface model is for further study.

network connection: A "transport entity" formed by the series of "connections" between "termination connection points".

originating PNO: An A PNO when it is also the initiating PNO. (This term was used in older versions of the specification).

Public Network Operator (PNO): An operator that manages an administrative ATM domain. The term PNO is used in the present document to be in alignment with EN 300 820-1 [1].

pnoVpSubnetwork: A subnetwork (according to ITU-T Recommendation G.805 [3]) is a topological component used for carrying ATM cells. PnoVpSubnetworks are delineated by termination points, modelled by vpCTPs contained in NWATMAccesspoints, and they are used for setting up pnoVpSubnetworkConnections.

NOTE: In principle (cf. to I-ETS 300 653) one subnetwork can consist of several subcomponents: subnetworks and connections between subnetworks (generally called link connections). But this capability is not supported in Xcoop. Usually one pnoVpSubnetwork represents an ATM network belonging to the domain one network operator.

protection switching: Automatic switching to pre-assigned spare capacity in network resources, consequent on reaction to receipt of an alarm signal by a network management system. (In the context of the present document, this is internal to a PNO).

recovery: Recovery is a procedure performed by a PNO which makes use of spare capacity in the subnetwork or inter-pno physical links belonging to this PNO. It follows after an alarm signal from a fault in the PNO's network resources.

star organization: It is described in EN 300 820-1 [1]. It is the organizational form that is used in this specification.

sub-network connection: A "transport entity" formed by a "connection" across a "sub-network" between "connection points". It can be configured as part of the "trail management process" as defined in ITU-T Recommendation G.805 [3].

subnetwork: A "topological component" used to effect routing and management. It describes the potential for "sub-network connections" across the "sub-network". It can be partitioned into interconnected "sub-networks" and "links". Each " sub-network" in turn can be partitioned into smaller "sub-networks " and "links" and so on. A "sub-network" may be contained within one physical node.

termination connection point: It is defined in ITU-T Recommendation G.805 [3].

trail: It is defined in ITU-T Recommendation G.805 [3].

transit PNO: A transit PNO is a PNO using its own subnetwork to perform its required transit part of VP connection. It has a provider role and corresponds to a leaf in the X-interface tree, not being the **Z** side. In the "cascaded/mixed approach" case (EN 300 820-1 [1]), it can be both a provider (where it acts as a transit) and a consumer (where it effectively acts as an Initiating PNO).

user: An end customer which is associated with the reservation of a VP connection.

VP subnetwork connection: A "transport entity" which is capable of transferring information transparently between "connection points" across a subnetwork or from a subnetwork access point to a user.

X-interface tree: With respect to a particular VP, an X-interface relationship exists between each provider PNO and its consumer PNO. Because each provider has exactly one consumer, the X-interface relations between all PNOs involved in the management of a particular VP form a tree, the X-interface relation tree. Note, that for a particular VP there can be several possible X-interface relation trees; the actual tree is formed at VP set-up. The root of the tree is the Initiating PNO; it uses (and via an X-interface controls) the PNOs (often transit PNOs), to which it is connected in the tree via its branches. The most right leaf of the tree is the Z PNO. Figure 1 shows an example of an X-interface tree.

X-interface: The management interface between two PNOs. In the "Responsibility Model", which is described in ITU-T Recommendation M.3010 [4], two Operations Systems Functions (= Managers) that are located in different TMNs (= different PNOs), communicate over an X Reference Point.

Z PNO: A Z PNO is a PNO whose subnet is connected to a user, where the overall VP connection ends.

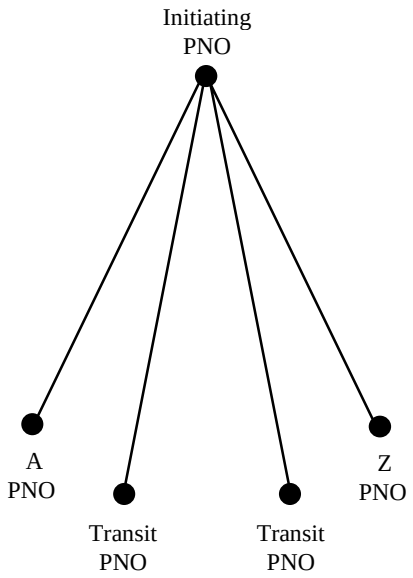


Figure 1: Example of an X-interface tree with the Initiating PNO not being the A PNO

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ATM	Asynchronous Transfer Mode
GDMO	Guidelines for the Definition of Managed Objects
MF	Management Functions
MFS	Management Function Sets
MS	Management Service
OS	Operation System
PNO	Public Network Operator
TMN	Telecommunications Management Network
VP	Virtual Path
VC	Virtual Channel

4 Requirements

F1 In case of faults, it should be possible to localize faults on a PNO sub-network and/or IPPL level.

F2 All parties which are affected by a faulty PNO sub-network are to be informed of the failure.

F3 All alarm information passed across the X-interface should be time-stamped.

F4 Elimination of redundant multiple alarms relating to a single underlying cause before the alarm information is transmitted across the X-interface.

F5 Protection switching and the result of the protection should be notified.

F6 It should be possible to enable/disable alarm reporting on a given connection or group of connections.

F7 It should be possible to modify the filtering criteria for alarm reporting.

5 Resources for ATM VP alarm management

5.1 The basis for the exchange of management information

The architectural framework characterizing the exchange of management information across the X-interface is represented in figure 2.

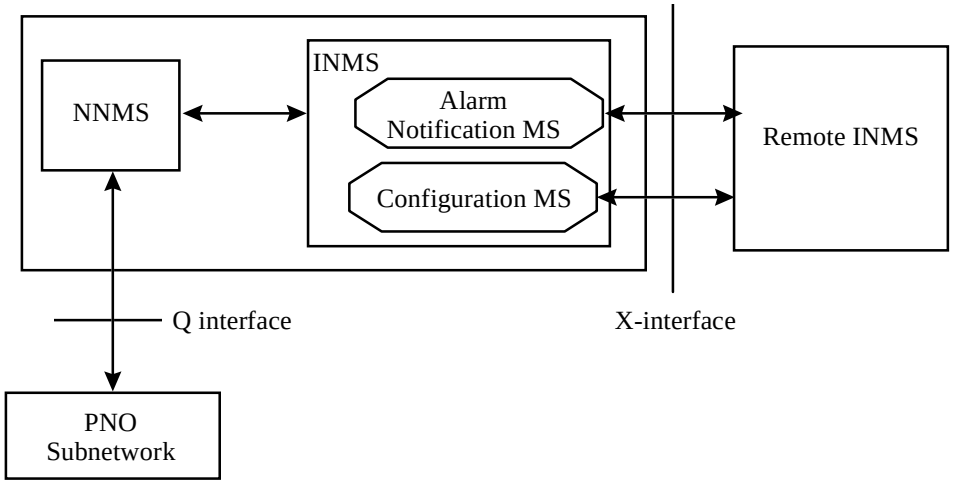


Figure 2: Architectural framework for the X-interface

In figure 2, the terms "NNMS" and "INMS" were derived from an earlier organizational point of view whereby administrations operated "National" (NNMS) and corresponding International (INMS) parts of a single overall network management system. For the present document these terms are retained but "INMS" can be assumed to be generalized to the management system for an X-interface interconnection between any two operators, whether within national boundaries or across them. NNMS can be assumed to be generalized to the internal management system of any operator which also relies on interconnections using X-interfaces.

The block named NNMS is responsible for the management of an operator's sub-network while the block named INMS is responsible for the management of connections between operators which in turn rely on interconnections with the operator's subnetworks. The distinction has been made because these two systems act on different Information Models and because there is the necessity of exchange of information between them. The logical positioning of the "Q" interface, which basically controls network switches in the NNMS, is also indicated but any matters relating to this interface are outside the scope of the present document.

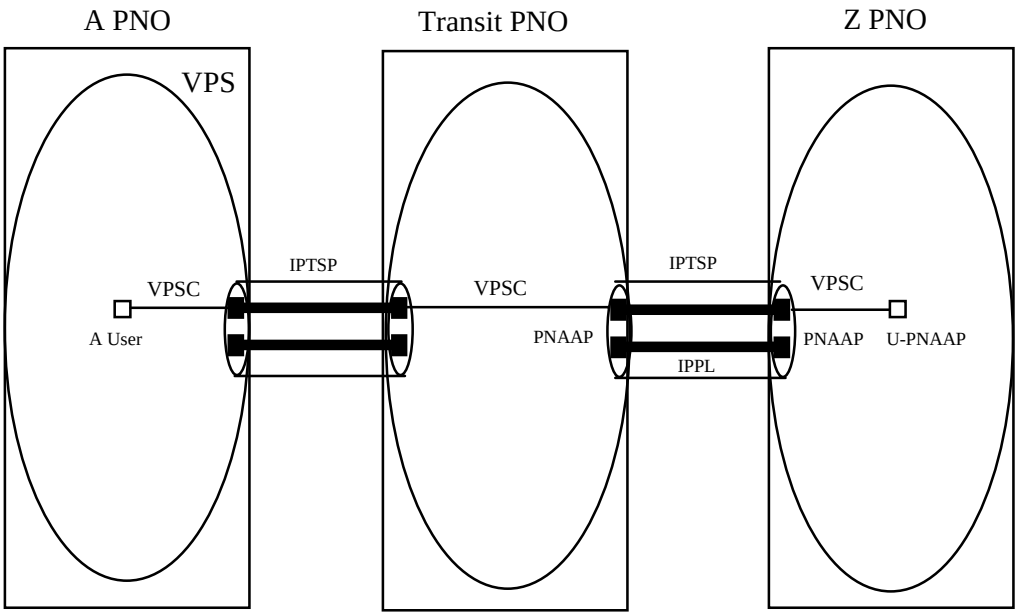
The INMS has to support the following operations as far as the Alarm Notification MS is concerned:

- reception of notifications coming from a remote INMS. These notifications are described in detail in subclause 7.1;
- reception of alarms coming from the NNMS and relevant to the X-interface. These alarms may be associated with faulty VP connections used for inter-network connections (they may be Physical Layer alarms or VP Layer alarms or faults affecting the ATM Cross Connect which acts as the inter-network gateway);
- elaboration of alarms coming from the NNMS (qualification and adaptation to inter-network alarm format);
- sending of alarms to the appropriate PNOs (Initiating PNO in the case of a VPSC fault or all PNOs in the case of Inter-PNO Physical Link (IPPL) fault);
- logging alarms and retrieving alarm reports.

5.2 The managed resources

A simplified view of the network level resources being managed is provided in figure 3.

An X-interface is presumed to exist at the management level between the PNOs shown in figure 3.



Legenda

VPS:	VP Subnetwork
VPSC:	VP Subnetwork Connection
IPTSP:	Inter-PNO Topological Subnetwork Pair
IPPL:	Inter-PNO Physical Link
PNAAP:	pnoNWatmAccessPoint
U-PNAAP:	pnoNWAtmAccessPoint for a user

Figure 3: X-interface managed network resources and connections

6 The VP alarm reporting management function sets

6.1 VP alarm reporting MS - Overview

In defining the VP Alarm Reporting MS for the X-interface and following the Ensembles concept, defined by the Network Management Forum NMF025 [10], some Management Function Sets (MFS) have been identified. Each MFS has been decomposed in MF. The following MFSs have been identified to manage the notifications described in clause 7:

- Alarm notification MFS;
- Alarm event logging MFS;
- Alarm processing MFS.

The identified VP Alarm Reporting MFSs are organized as depicted in figure 4 and described in more detail in subclauses 6.2, 6.3 and 6.4.

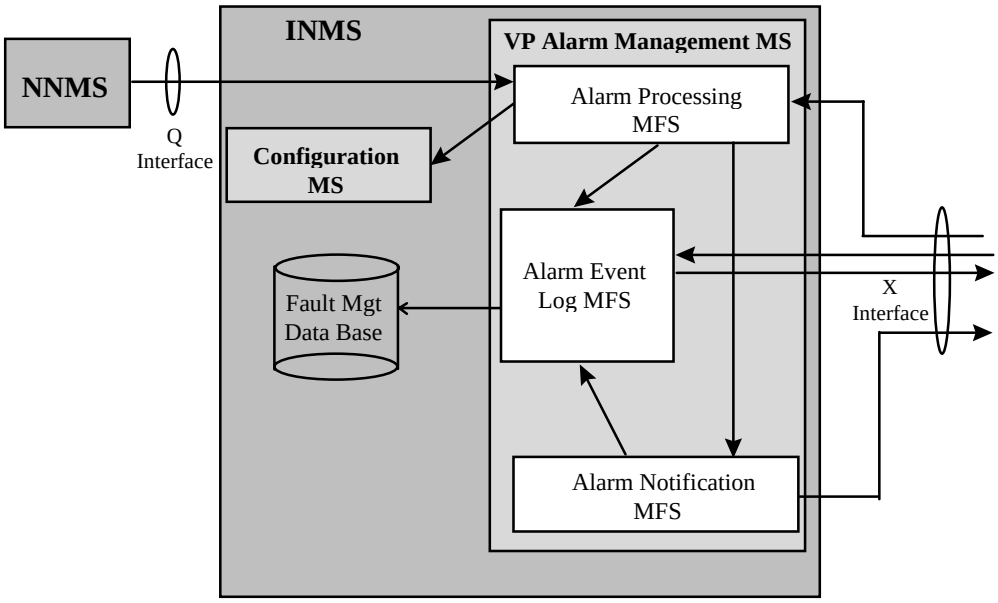


Figure 4: MFSs relative to the VP alarm management MS

6.2 Alarm notification MFS

This MFS performs the following tasks:

transmission of faulty VP alarm notifications across the X-interface; these notifications contain the following parameters:

SubnetworkId, resource id (vpConnectionId, atmAccessPointId), time of event, probable cause, perceived severity, specific problems (the last three of which are described in more detail below and are derived from the event information section of ITU-T Recommendation X.733 [6] and are reproduced here in order to clarify the basis on which the MFS messages are generated by the system).

forwarding of sent alarms to the Alarm Event Logging MFS to be recorded in the SALog:

The four types of Alarm Notifications are summarized in figure 5. In the case of an IPPL failure the same notifications are sent but to all PNOs instead of only the Origin PNO.

probableCause: This parameter defines further qualification (after Event Type and information) as to the probable cause of the alarm. Probable cause values for notifications shall be indicated in the behaviour clause of the object class definition. The syntax of standard probableCauses shall be the ASN.1 type object identifier. The managed object class designer should choose the most specific probableCause applicable.

The set of probableCauses will not be further elaborated here and reference should be made to ITU-T Recommendation X.733 [6].

specificProblems: This parameter identifies the status of the alarm in the VP Alarm MS. In the context of these specifications, the specificProblems values have been restricted to:

- protection-switched;
- under-recovery;
- cleared;
- unrecoverable.

perceivedSeverity: This parameter defines six severity levels, which provide an indication of how it is perceived that the capability of the managed object has been affected. Briefly, these are:

- **cleared:** Indicates the clearing of one or more previously reported alarms.

- **indeterminate:** Indicates that the severity level cannot be determined.
- **critical:** Indicates that a service affecting condition has occurred and an immediate corrective action is required.
- **major:** Indicates that a service affecting condition has happened and an urgent corrective action is required.
- **minor:** Indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.
- **warning:** Indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt.

Again, reference should be made to ITU Recommendation X.733 [6] for full descriptions.

6.3 Alarm processing MFS

For the Alarm Processing MFS the following tasks are identified:

- With regard to the NNMS interface (Not a part of the X-interface specification):
  - **reception** of alarms concerning the part of the PNO's NNMS-based sub-network supporting INMS-based connections. It is assumed that these alarms are "qualified" in the sense that the recognition of repeating alarms and the measurement of persistence has been already performed by the NNMS;
  - **adaptation** of the NNMS-based alarm to the required INMS format. This adaptation will allow the same treatment for NNMS-based and INMS-based alarms;
  - **forwarding** the INMS alarms (i.e. the NNMS alarms that have been adapted to INMS format and that shall be sent to other PNOs) to the VP Alarm Notification MFS.
- With regard to the INMS Interface:
  - **reception of alarms from remote INMSs** across the X-interface; the alarm indications will contain the following parameters: Subnetwork Id (Sub-network whose PNO has detected the Fault), affected resource id (VPconnectionId, pnoNWAtmAccessPoint, ...), time of event, probable cause, perceived severity, and specific problems. It is supposed that the Sub-network has performed recognition of repeating alarms and measurement of persistence before issuing the alarm across the X-interface. The end of the alarm event will be communicated by using the same alarm indication with the perceived severity field set to "cleared";
  - **forwarding** the received alarms to the RA Log to be stored.
- Filtering:
  - **discrimination and failure localization**: it localizes the failure on the basis of the information received. The PNO which receives one or more alarm notifications coming from other PNOs will be capable of distinguishing the cause of the fault from the inducing causes by analysing the alarm notification parameters.

The alarm notification is logged in RAlog (see alarm event logging MFS).

6.4 Alarm event logging MFS

This task is in charge of managing the interactions with the logs. Logging of alarms may be organized as follows:

- RALog: log of received alarms from remote INMSs, recorded sequentially;
- QALog: is a log which records the qualified alarms, storing begin, end, counting of alarm repetitions;
- SALog: log of sent alarms across the X-interface. This log (and only this type) may also be viewed from a remote INMS.

Therefore this MFS performs the following tasks:

writing alarms that are generated by the Alarm Processing MFS and the Alarm Notification MFS. This function records the next alarm events:

- the ones that qualify as alarms (with regard to number of occurrences, persistence, etc.). The set of these alarms are summarized under the concept "QALog". (QALog is not visible over the X-interface);
- alarm notifications that arrive from the X-interface (these are summarized under RALog, which is not visible over the X-interface);
- the alarm notifications that are transmitted over the X-interface. (these are recorded in the SALog, which is visible over the X-interface).

reading information (not a part of the X-interface specification) contained in the logs upon request by the operator. This function accesses the SALog, RALog and QALog in order to read alarm records. Some access keys may be identified for accessing the information stored in the logs.

request alarm report: this function is performed (over the X-interface) when an INMS wants to read the SALog of a remote INMS. The output of this function is the Alarm Record retrieved from the INMS of the remote PNO by the requesting INMS. It is supposed here that the requesting INMS will specify a set of characteristics of the alarm in order to get the proper Alarm Record.

The IPPL alarm-logs should be readable by all PNOs in the system. The VPSC alarm-logs should be readable only for the PNO that requested the connections involved (The I PNO).

The identified MF across the X-interface is the function described in clause 7.

7 Management functions

7.1 Alarm notification management functions

(The structure of the Alarm notifications should be in accordance with ITU-T Recommendation X.733 [6]. For reading the proper alarm record the use of filters specified in ITU-T Recommendation X.711 [11] may be required).

a) to h) describe the MFs composing the MFS:

a) MF: Notification of VP Sub-network Connection Protection Switching

MF Name	Notification of VP Sub-network Connection Protection Switching
Functionality	This function generates the emission of a VPSC Protection Switching notification across the X-interface. This is done in consequence of having received from the NNMS an indication of a protection switching action affecting a PNO's sub-network protected resources supporting inter-PNO communications. The notification is emitted towards the Initiating PNO by the **pnoVpSubnetworkConnection** object.
Object class	pnoVpSubnetworkConnection
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId vpConnectionId
Request/parameters	time of event probableCause specificProblems = protection-switched perceivedSeverity = warning
Response/parameters	not confirmed
Security	Writes in the SALog

b) MF: Notification of Inter-PNO Physical Link Protection Switching

MF Name	Notification of Inter-PNO Physical Link Protection Switching
Functionality	This function generates the emission of an IPPL Protection Switching notification across the X-interface. This is done by the responsible PNO in consequence of having received from the NNMS an indication of performing a protection switching procedure on a protected link affected by a recoverable failure. The notification is emitted towards every PNO by the **pnoNWAtmAccessPoint** object.
Object class	pnoNWAtmAccessPoint
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId pnoNWAccessPointId
Request/parameters	time of event probableCause specificProblems = protection-switched perceivedSeverity = warning
Response/parameters	not confirmed
Security	Writes in the SALog

c) MF: Notification of VP Sub-network Connection Under Recovery

MF Name	Notification of VP Sub-network Connection Under Recovery
Functionality	This function generates the emission of a VPSC Under Recovery notification across the X-interface. This is done in consequence of having received from the NNMS an indication of a recovery action affecting the PNO's sub-network resources supporting inter-PNO communications. This notification is sent by the **pnoVpSubnetworkConnection** object to the Initiating PNO.
Object class	pnoVpSubnetworkConnection
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId vpConnectionId
Request/parameters	time of event probableCause specificProblems = under-recovery perceivedSeverity = critical OR major OR minor OR warning OR indeterminate (i.e. any valid severity value except "cleared").
Response/parameters	not confirmed
Security	Writes in the SALog

d) MF: Notification of Inter-PNO Physical Link Under Recovery

MF Name	Notification of Inter-PNO Physical Link Under Recovery
Functionality	This function consists in the emission of an IPPL Recovery notification across the X-interface. This is done by the PNO responsible for the link in consequence of the detection of a recoverable failure affecting the link. This notification is sent by the **pnoNWAtmAccessPoint** object to all the PNOs.
Object class	pnoNWAtmAccessPoint
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId pnoNWAccessPointId
Request/parameters	time of event probableCause specificProblems = under-recovery perceivedSeverity = critical OR major OR minor OR warning OR indeterminate (i.e. any valid severity value except "cleared")
Response/parameters	not confirmed
Security	Writes in the SALog

e) MF: Notification of VP Sub-network Connection Recovery Result

MF Name	Notification of VP Sub-network Connection Recovery Result
Functionality	This function generates the emission of a VPSC Recovery Result notification across the X-interface. This is emitted after having received from the NNMS an indication of the recovery procedure results. This notification is sent by the **pnoVpSubnetworkConnection** object to the Initiating PNO.
Object class	pnoVpSubnetworkConnection
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId vpConnectionId
Request/parameters	specificProblems = cleared OR unrecoverable perceivedSeverity = cleared OR if specificProblems = unrecoverable then any valid value except "cleared" (but must be the same as for the corresponding Under Recovery notification)
Response/parameters	not confirmed
Security	Writes in the SALog

f) MF: Notification of Inter-PNO Physical Link Recovery Result

MF Name	Notification of Inter-PNO Physical Link Recovery Result
Functionality	This function generates the emission of an IPPL Recovery Result notification across the X-interface by the responsible PNO. This is done in consequence of having received the recovery procedure results about the affected link. This notification is sent by the **pnoNWAtmAccessPoint** object to all the PNOs.
Object class	pnoNWAtmAccessPoint
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId pnoNWAccessPointId
Request/parameters	specificProblems = cleared OR unrecoverable perceivedSeverity = cleared OR if specificProblems = unrecoverable then any valid value except for cleared (but must be the same as for the corresponding Under Recovery notification)
Response/parameters	not confirmed
Security	Writes in the SALog

g) MF: Notification of VP Sub-network Connection Unrecoverable

MF Name	Notification of VP Sub-network Connection Unrecoverable
Functionality	This function generates the emission of a VPSC Failure Indication notification across the X-interface. This is done in consequence of having received from the NNMS an indication of a fault affecting a PNO's sub-network resources supporting inter-PNO communications which are non protected or no recovery procedure is available. This notification is sent by the **pnoVpSubnetworkConnection** object to the Initiating PNO which might decide to interrupt the service.
Object class	pnoVpSubnetworkConnection
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId vpConnectionId
Request/parameters	specificProblems = Unrecoverable time of event probableCause perceivedSeverity = critical/major/minor/warning/indeterminate (i.e. any valid severity value except "cleared")
Response/parameters	not confirmed
Security	Writes in the SALog

h) MF: Notification of Inter-PNO Physical Link Unrecoverable

MF Name	Notification of Inter-PNO Physical Link Unrecoverable
Functionality	This function consists in the emission of an IPPL Unrecoverable Failure notification across the X-interface. This is done by the responsible PNO in consequence of having received an indication of an unrecoverable failure. This notification is sent by the **pnoNWAtmAccessPoint** object to all PNOs which are then expected to update their topology information.
Object class	pnoNWAtmAccessPoint
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId pnoNWAccessPointId
Request/parameters	time of event probableCause specificProblems = Unrecoverable perceivedSeverity = critical/major/minor/warning/indeterminate (i.e. any valid severity value except "cleared")
Response/parameters	not confirmed
Security	Writes in the SALog

Figure 5 illustrates the use of the Alarm notification actions and X-interface messages, followed by some additional explanation.

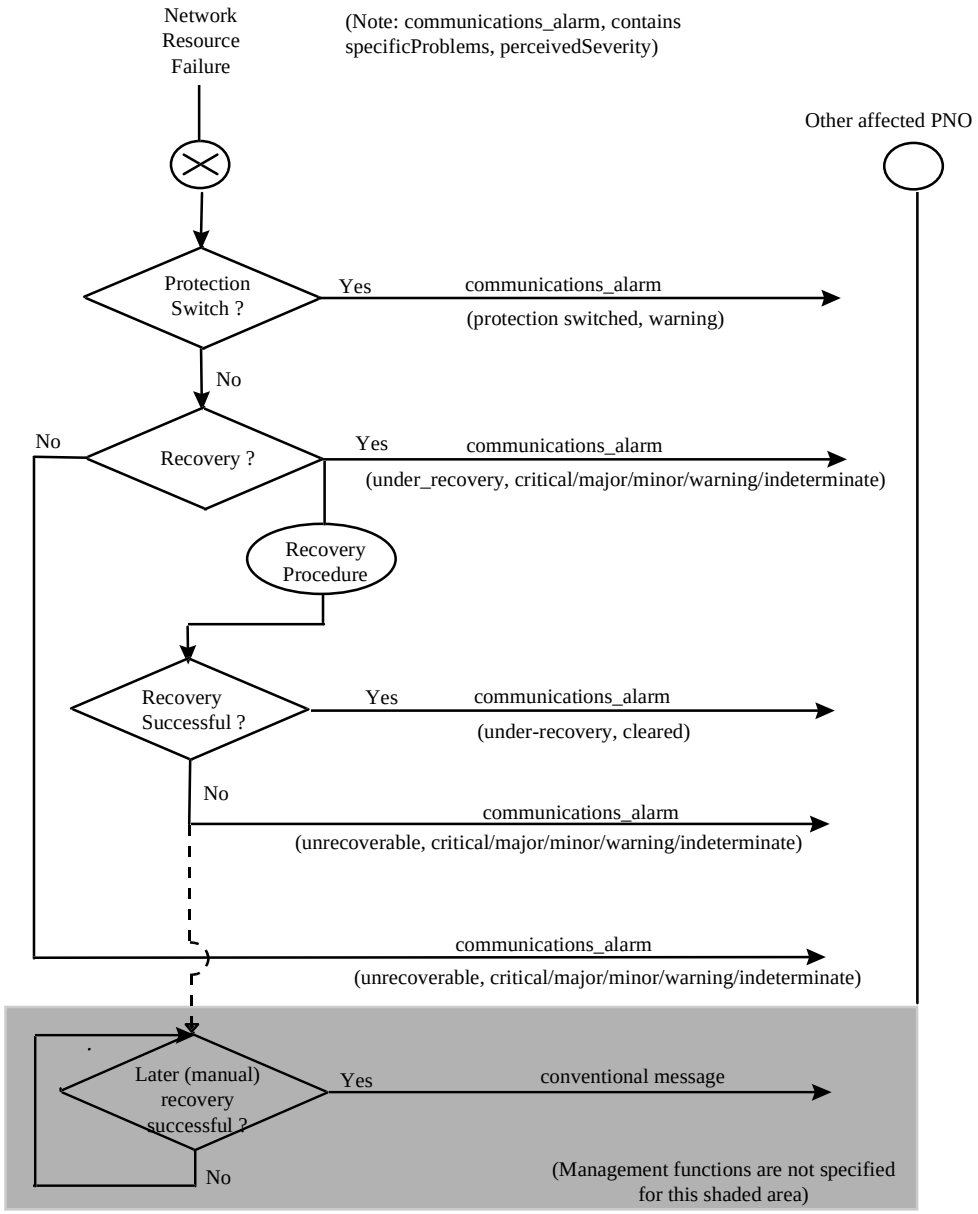


Figure 5: Alarm notification management messages and actions

Figure 5 shows the sequence of actions and Alarm management messages which occur in consequence of the reception of a network resource failure message relating to the resources of that particular PNO which is a provider to any operational VP. The following describes the actions and messages.

An alarm signal is emitted from a switch or other network resource. (Such a signal will probably originate from either a fault or from a performance degradation).

Communications_alarms are emitted as indicated by the horizontal arrows shown in shown in figure 5.

Firstly, the affected PNO will be presumed to attempt to rectify the associated fault by automatically switching to pre-assigned spare capacity which is defined as "Protection Switching (PS)" within the scope of the present document. This is notified (across the X-interface) by emission of the communications_alarm, protection switched_warning.

Secondly, if such PS is unavailable or fails, the system will then go into an attempted recovery procedure.

If there is no recovery procedure available, a communications_alarm, unrecoverable is emitted immediately.

If a recovery procedure is available, a communications_alarm, under_recovery is emitted immediately. This is followed by the Recovery Procedure actions. At the completion of these actions a further communications_alarm is emitted. This will either report that the fault is cleared or that the fault is unrecoverable.

Consequent on receipt of an unrecoverable failure message, the Initiating PNO could be expected to wish to reconfigure the VP service, EN 300 820-1 [1].

The grey box in figure 5 is indicative of a requirement for the PNO owning the faulty network resource to (presumably) need to repair or replace this by manual means. Reporting the availability of such repaired or replaced resources is not part of this X-interface specification. A PNO may, however, choose to report the manual resource recovery by conventional means and is then able to use these resources again to respond to X-interface reservations, EN 300 820-1 [1].

7.2 Alarm processing management function

The following function performs the alarm processing MFS across the X-interface:

MF: Alarm reception

MF Name	Alarm Reception
Functionality	This function receives alarm notifications sent by remote PNOs across the X-interface.
Object class	vpSubNetworkConnection OR pnoNWAtmAccessPoint
Notifications	"ITU-T Recommendation X.721 [5]": communicationsAlarm
Instance values	subNetworkId subNetworkId OR pnoNWAccessPointId
Request/parameters	Time of Event Probable cause Perceived severity Specific Problems
Response/parameters	not confirmed
Security	Writes in the RALog

7.3 Alarm event logging management function

The following function performs the alarm event logging MFS across the X-interface:

(The structure of the alarm should be in accordance with ITU-T Recommendation X.733 [6]).

MF: Request alarm report

MF Name	Request alarm report
Functionality	This function consists of the emission of a read message across the X interface requesting a remote INMS about an alarm in the SALog. The message sent through the X-interface is a GET request on the **log** object.
Object class	log
Action	get
Instance values	subNetworkId, logId
Request/parameters	Access Key (It could be the remote subNetworkId, the pnoNWAtmAccessPointId, vpConnectionId, Probable cause, Perceived severity etc.)
Response/parameters	alarmRecord attribute values
Security	Access (only read) to SAlog

8 Scenarios

To clarify the exchange of messages across the X-interface, two scenarios are considered: the first usage case relates to when a failure occurs within a sub-network and the second usage case relates to when a failure occurs on a physical link between two PNO's sub-networks.

Case 1

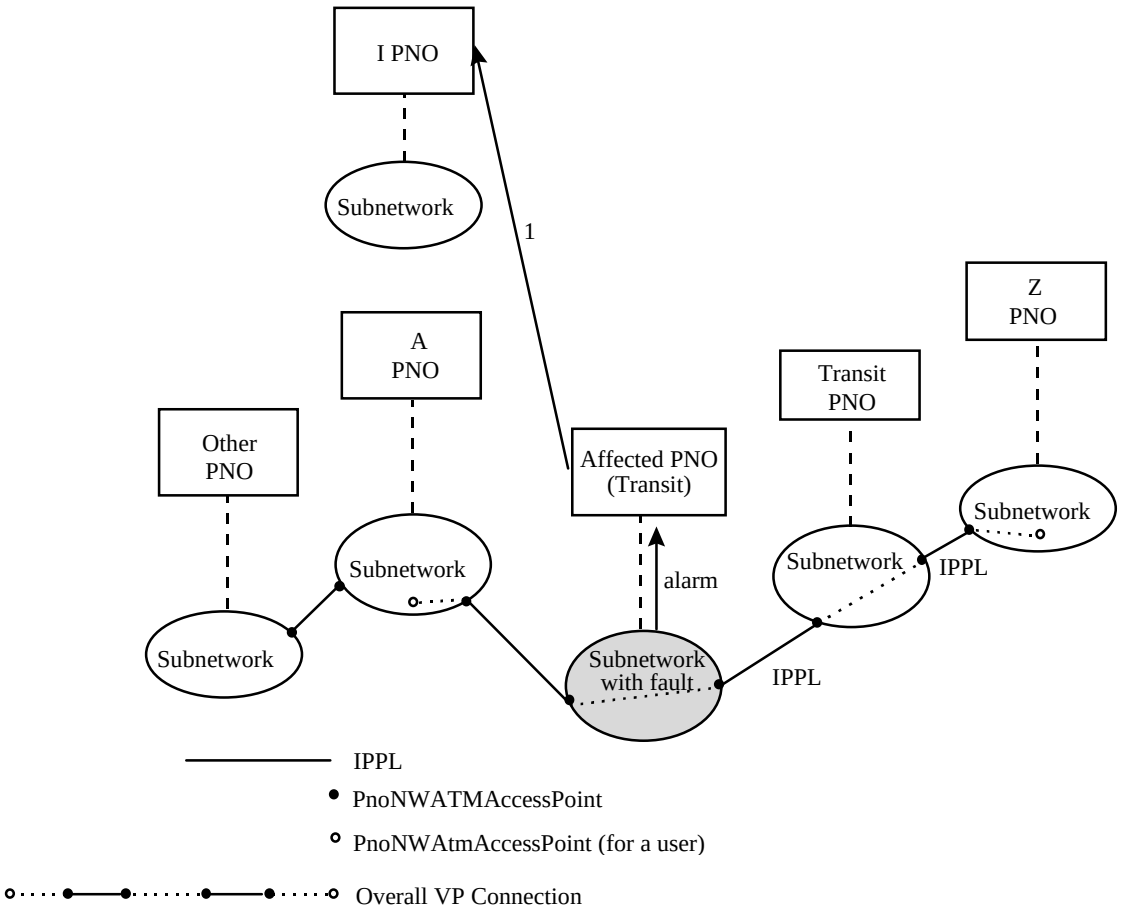


Figure 6: Alarm reporting management when a sub-network fails

If a sub-network fails, its INMS (**alarm management**) should inform the PNOs which are initiating PNOs of the VP sub-network connections that cross the faulty Sub-network. Figure 6 represents the alarm reporting process in the case that just one VP sub-network connection makes use of the faulty sub-network resources. (In this figure, the initiating PNO is not the A PNO). In this case a VPSC notification is sent to the one initiating PNO indicated. Clearly, the process would have to be repeated "n" times for "n" different subnetwork connections using the faulty sub-network at the time of failure.

Case 2

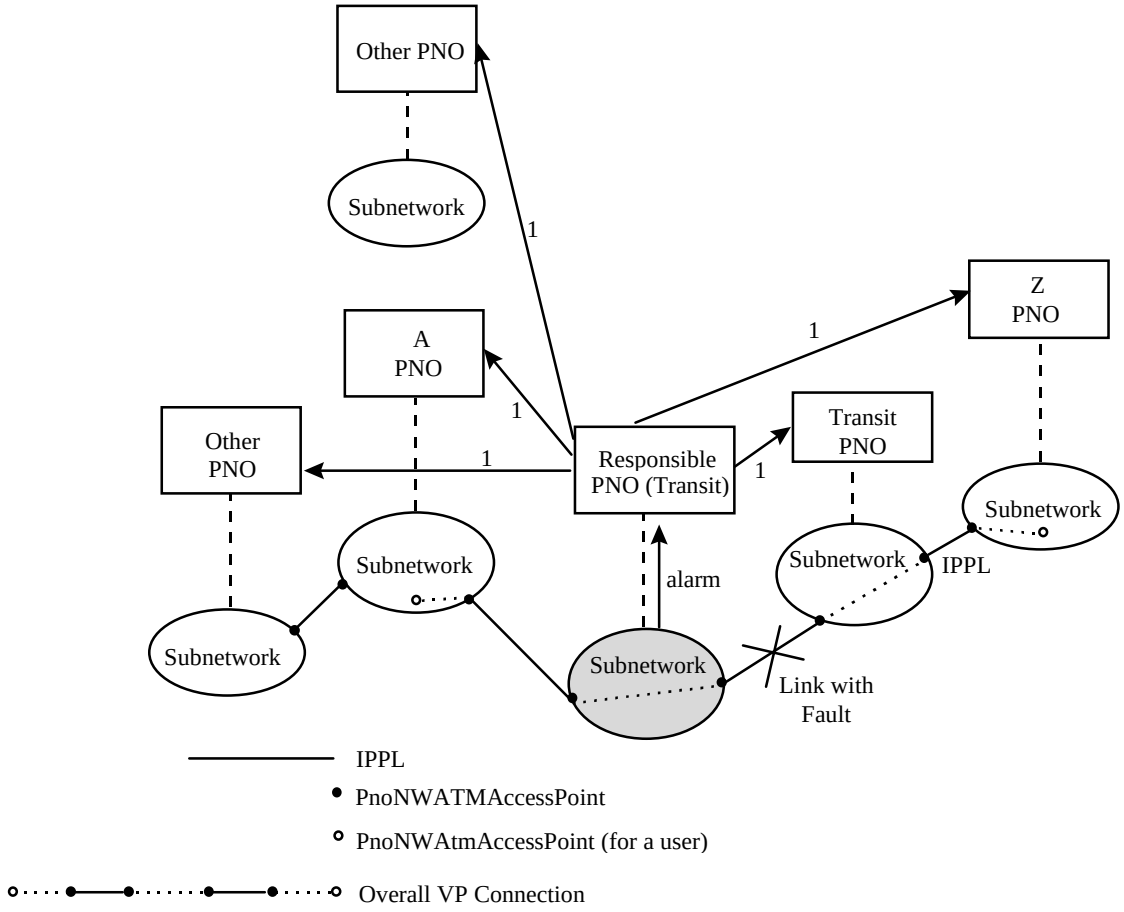


Figure 7: Alarm reporting management when an Inter-PNO Physical Link fails

Each IPPL should have a PNO assigned as responsible in terms of its **alarm management**. It is presumed that this assignment will be by bilateral agreements pending the availability of standardization on this issue.

If an IPPL fails, only the "responsible" one of the two PNOs connected by the link should forward the associated failure notification through the X-interface.

The responsible PNO informs all the other PNOs in the X-interface system about the **alarm management** process of the Inter PNO Physical Link, even if they have no VP connection in common. The reason for informing all the PNOs is that the Topology Information of each PNO should be updated. This is especially important in case of an unrecoverable failure when a corresponding unrecoverable failure notification is sent to all PNOs in the international network scheme where management is undertaken using the X-interface.

9 Management information

9.1 Relationships

This subclause lists the Managed Objects, Inheritance Tree and Naming Tree relating to the ATM VP **alarm management** X-interface. A relationship can also be drawn with respect to ITU-T Recommendation M.3400 [7] and the ITU-T Recommendation X.7xx series.

9.1.1 Managed objects

For the purpose of defining alarm reporting functions the necessary resources are described as follows:

pnoVpSubnetworkConnection: It represents a VP connection across a PNO sub-network. This connection is seen by the Origin PNO as a whole, with no details regarding the way the connection is composed inside the PNO domain.

pnoNWAtmAccessPoint: It represents the access point to the ATM PNO Sub-network, or in other words, it represents an endpoint of a physical link at the cell level between two PNOs. Each IPPL is terminated by two pnoNWAtmAccessPoints which are in charge of emitting alarm notifications when detecting failures related to the link or to the access point itself.

Log: Described in ITU-T Recommendation X.721 [5]. Each PNO can implement up to three logs in its VP Alarm Reporting Management system. These are the "Sent Alarm (SA)", Qualified Alarm (QA) and Received Alarm (RA) Logs respectively. Only the SA Log is visible over the X-interface and mandatory. It allows the other PNOs to consult the events sent by the affected PNO. (The other two logs are optional and not visible over the X-interface. Briefly, the RA Log will record alarms received over the X-Interface and the QA Log will be used to collect alarms and ensure avoidance of alarm persistence and duplication).

eFD: Described in ITU-T Recommendation X.721 [5]. It is not visible over the X-interface but its functionality - or a comparable one is needed to send the events through the X-interface.

alarmRecord: Described in ITU-T Recommendation X.721 [5] for alarm event logging.

objectCreationRecord: Described in ITU-T Recommendation X.721 [5] for logging the creation of objects.

objectDeletionRecord: Described in ITU-T Recommendation X.721 [5] for logging the deletion of objects.

stateChangeRecord: Described in ITU-T Recommendation X.721 [5] for logging changes of state attributes.

attributeValueChangeRecord: Described in ITU-T Recommendation X.721 [5] for logging changes of attributes values.

9.1.2 Inheritance tree

The inheritance tree of the log objects is shown in figure 8.

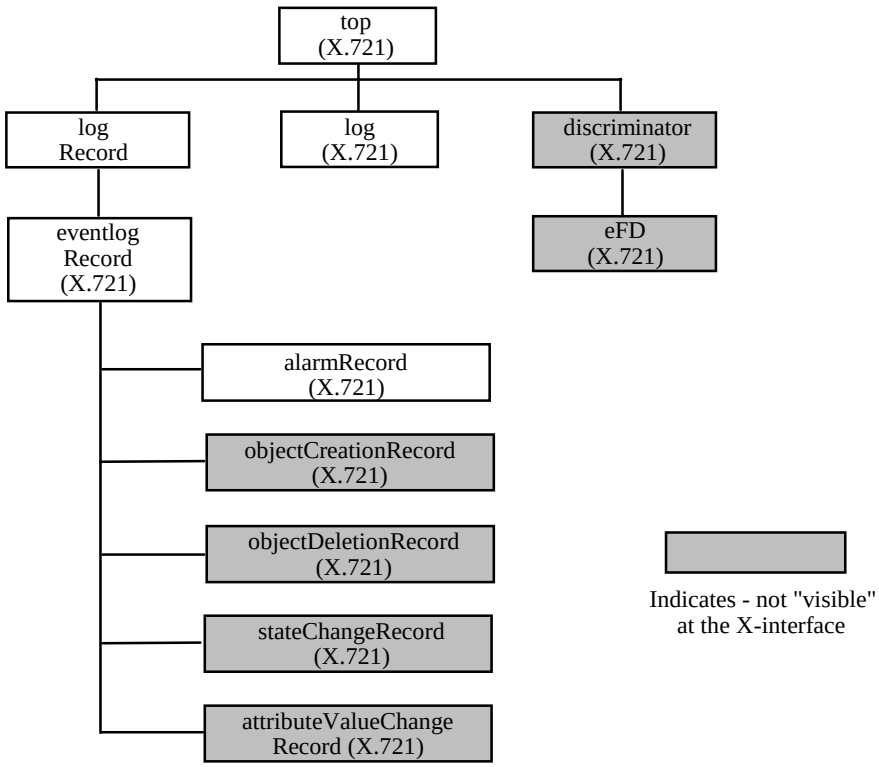


Figure 8: Inheritance tree

9.1.3 Naming tree

To fulfil the MSs described in clause 6, the object classes shown in the Naming tree in figure 9 are used. The next subclause details this Information Model in GDMO and ASN.1 terms.

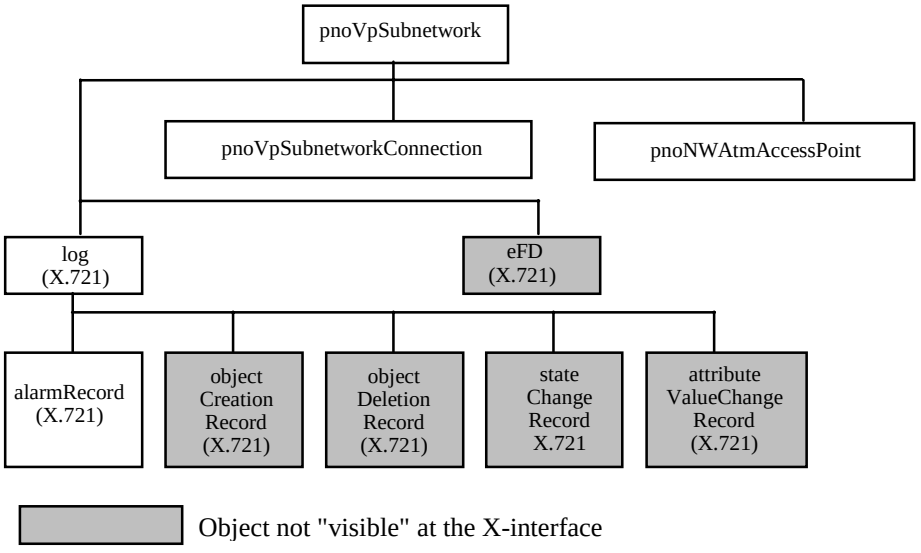


Figure 9: Naming tree

IPPL failures are related to the pnoNWAtmAccessPoint object class while the VPSC failures relate to the pnoVpSubnetworkConnection object class. Accordingly, it is necessary to include both object classes in the naming tree.

The log object class represents the complete set of alarm records without specifically distinguishing for pnoVpSub-networkConnection and for pnoNWAtmAccessPoint.

The discriminatorConstruct attribute (type defined as CMISE Filter) of the dedicated log object instance(s) has to be set in accordance with the required event reports (Alarm Notifications) received across the X-interface to enable the creation of the corresponding object instances of eventLogRecord subclasses. This approach covers the requirements for RALog Records.

Read access to the Sent Alarm log records across the X-interface of any PNO could be enabled by setting the authorization profiles accordingly.

In the present document, a PNO is not obliged to allow other PNOs the control over the forwarding of events across the X-interface. This event-forwarding is controlled by the Agent locally, which is in accordance with ITU-T Recommendation X.734, annex B.1 [8].

Therefore, in this specification, an Agent is not obliged to use an eFD (X.721: eventForwardingDiscriminator, ITU-T Recommendation X.721 [5]) to send Notifications over the X-interface, and thus the eFD needs not to be visible over the X-interface.

However, its functionality -or a comparable one- is needed within the alarm management System for sending the different alarm management messages, as described in clause 7 Alarm notification.

The notifications crossing the X-interface are described in the alarm management specification normally within the behaviour description of the object classes. The parameters contained in these notifications are also defined.

NOTE: The following information could be used for implementation.

The requirements for SALog Records are covered by setting the discriminatorConstruct attribute of the dedicated eventForwardingDiscriminator object instance(s) in accordance with the required event reports (Alarm Notification) to be sent across the X-interface. The event reports then can be logged, forwarded or displayed by the adjacent OS.

The requirements of QALog Records could be covered in the same way as the sent/received records.

9.2 X-interface GDMO description

For the GDMO description refer to EN 300 820-1 [1].

9.3 X-interface ATM VP alarm management ASN.1 module

The ASN.1, ITU-T Recommendation X.208 [9], module below provides an abstract syntactical description of the X-interface GDMO. As such, it gives an implementation and platform independent description of the object classes required in the interface definition.

```
ASN1XatmVpNotificationModule { ccitt(0) identified-organization(4) etsi(0) ETS300820-2(8202)
informationModel(0) asn1Module(2) asn1TypesModule(0) }

DEFINITIONS

BEGIN

IMPORTS SpecificProblems, SpecificIdentifier

FROM {joint-iso-ccitt ms(9) smi (3) part2(2) asn1Module(2) 1};

xfSpecificProblems OBJECT IDENTIFIER ::= { ccitt(0) identified-organization (4) etsi (0) ETS300820-2
(8202) informationModel(0) specificExtension(0) xialarm (0) }

cleared SpecificProblems ::= globalValue: { xfSpecificProblems 0}

protectionSwitched SpecificProblems ::= globalValue: { xfSpecificProblems 1}

under-recovery SpecificProblems ::= globalValue: { xfSpecificProblems 2}

unrecoverable SpecificProblems ::= globalValue: { xfSpecificProblems 3}

END
```

Annex A (informative): Security aspects

With regard to access control as seen from a particular PNO's point of view the next table should be considered:

Object class	Access to the instances in accordance with the GDMO definition of the Object Class for:	Alarm Notifications are sent to:
pnoVpSubnetworkConnection	See EN 300 820-1 [1]	Only the PNO that requested the creation of the instances involved. (Initiating PNO)
pnoNWAtmAccessPoint	See EN 300 820-1 [1]	All other PNOs
alarmRecord, regarding pnoVpSubnetworkConnection-alarms.	Only the PNO that requested the creation of the pnoVpSubnetworkConnection instances involved. (Initiating PNO) (note 1)	-
alarmRecord, regarding pnoNWAtmAccessPoint-alarms.	All PNOs	-
log	Only GET on logId allowed (note 2)	-

NOTE 1: A Manager, trying to read from alarmRecord all Instances that regard pnoVpSubnetworkConection-alarms shall only get the Instances in which he is the initiating PNO. Whether his attempt to read all instances should be registered is a matter for "Security Management".

NOTE 2: OC log is not manageable over the X-interface, it is used as base for scoped GETs only.

In general, the usage of a "closed user group" is suggested; only PNOs that are in the closed user group are allowed to set up an association with the appropriate PNO.

How this access control is implemented is not within the scope of the present document.

History

Document history				
V1.2.1	October 1997	Public Enquiry	PE 9807:	1997-10-17 to 1998-02-13
V1.2.3	April 1998	Vote	V 9826:	1998-04-28 to 1998-06-26
V1.2.3	July 1998	Publication		

ISBN 2-7437-2369-6
Dépôt légal : Juillet 1998