Draft ES 201 097-1 V1.1.1 (1997-10)

ETSI Standard

Network Aspects (NA); Telecommunications Management Network; Resource Management Part 1: Physical Resource Management

European Telecommunications Standards Institute

Reference
DES/NA-043320 (a5o90icp.PDF)

Keywords
Management

ETSI Secretariat

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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

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

Contents

Foreword

This ETSI Specification (ES) has been produced by ETSI Technical Committee Network Aspects (NA), and is now submitted for the ETSI standards Membership Approval Procedure (MAP).

Introduction

General description

To deal with the complexity of telecommunications management, the management functionalities may be considered to be partitioned into logical layers. A logical layer reflects particular aspects of management and implies the clustering of management information supporting that aspect (ITU-T Recommendation M.3010 [11]).

The grouping of management functionalities implies grouping Operations System Functions (OSFs) based upon business, service, network and element layers. The element OSFs and network OSFs share the infrastructure aspects of a telecommunications network. The OSFs provide the functionality to manage a network by co-ordinating activities across the network.

The present document relates to the management of physical resources and does not specify objects relating to a single interface. Physical resource management functionalities may be split between the element OSF and the network OSF.

The management of physical resources may be applicable to the following interfaces:

- Network Layer OS to Network Element Management Layer (NEML) OS;
- Network Element Management Layer OS to the Network Element (NE).

The physical resources may belong to technologies such as switching, access transmission, etc.

Relationship with other standards

The present document has been developed according to the TMN interface specification methodology defined in ITU–T Recommendation M.3020 [12]. The functional description of the physical resource management (functional requirements and management functions) is based on ITU-T Recommendation M.3400 [8]. All applicable OSI Systems Management Functions (SMF) (ITU-T Recommendation X.7 series) are reused.

The information model is fully aligned with ITU-T Recommendation M.3100 [13]. Backward compatibility for models which are based on ITU-T Recommendation M.3100 [13] is also supported.

Blank page

1 Scope

The resource management series of standards relates to the generic model for the management of NE resources (hardware and software). It provides the managed objects to be applicable at both these OS-NE and OS-OS interfaces. It is partitioned into a number of parts of which this is part 1.

The present document defines a generic information model for physical resource management. The information model and its relationship with physical resources such as equipment, slots, subracks, racks etc. are defined. Managed objects are provided that cover a number of management requirements and functions, concerning the configuration and fault management functional areas.

The scope of the present document includes:

- Fault management functional area:
  - Alarm surveillance;
  - Log control;
  - Fault localization;
  - Fault correction;
  - Testing.
- Configuration management functional area:
  - Installation;
  - Provisioning;
  - Status and control.

The present document does not:

- define the nature of any implementation intended to provide the physical resource management functions;
- specify the manner in which management is accomplished by the user of the physical resources management functions;
- specify the services necessary for the establishment, normal and abnormal release of a management association;
- specify conformance proformas.

2 Normative references

The present document incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to the present document only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETSI EN 301 251 (1996): "Digital cellular telecommunications system (Phase 2); Fault management of the Base Station System (BSS) (GSM 12.11version 4.1.1)".

[2] ETSI ETS 300 119-1 (1994): "Equipment Engineering (EE); European telecommunication standard for equipment practice; Part 1: Introduction and terminology".

[3] ETSI ETS 300 119-2 (1994): "Equipment Engineering (EE); European telecommunication standard for equipment practice; Part 2: Engineering requirements for racks and cabinets".

[4] ETSI ETS 300 119-3 (1994): "Equipment Engineering (EE); European telecommunication standard for equipment practice; Part 3: Engineering requirements for miscellaneous racks and cabinets".

[5] ETSI ETS 300 119-4 (1994): "Equipment Engineering (EE); European telecommunication standard for equipment practice; Part 4: Engineering requirements for subracks in miscellaneous racks and cabinets".

[6] ETSI ETS 300 304 Ed.2 (1997): "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); SDH information model for the Network Element (NE) view".

[7] ETSI RE/TM 2213-1 Version 3 (1996): "Transmission and Multiplexing - Maintenance of the ETS 300 304 Edition 2".

[8] ITU-T Recommendation M.3400 (1996): "Maintenance: telecommunications management network. TMN management functions".

[9] ITU-T Recommendation G.774-03 (1994): "General aspects of digital transmission systems. Synchronous digital hierarchy (SDH) management of multiplex section protection for the network element view".

[10] ITU-T Recommendation G.803 (1993): "Digital networks. Architecture of transport networks based on the synchronous digital hierarchy (SDH)".

[11] ITU-T Recommendation M.3010 (1992): "Maintenance: telecommunications management network. Principles for a telecommunications management network".

[12] ITU-T Recommendation M.3020 (1992): "Maintenance: telecommunications management network. TMN interface specification methodology".

[13] ITU-T Recommendation M.3100 (1995): "Maintenance: telecommunications management network. Generic network information model".

[14] ITU-T Recommendation Q.821 (1993): "Specification of signalling system No. 7 - Q3 interface. Stage 2 and Stage 3 description for the Q3 interface - Alarm surveillance".

[15] ITU-T Recommendation X.208 (1988): "Data communication networks - Open systems interconnection (OSI) model and notation, service definition: Specification of Abstract Syntax Notation One (ASN.1)".

[16] ITU-T Recommendation X.680 (1994): "Data networks and open system communication - OSI networking and system aspects - Abstract Syntax Notation One (ASN.1). Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[17] ITU-T Recommendation X.681 (1994): "Data networks and open system communication - OSI networking and system aspects - Abstract Syntax Notation One (ASN.1). Information Technology - Abstract Syntax Notation One (ASN.1): Information object specification".

[18] ITU-T Recommendation X.682 (1994): "Data networks and open system communication - OSI networking and system aspects - Abstract Syntax Notation One (ASN.1). Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification".

[19] ITU-T Recommendation X.683 (1994): "Data networks and open system communication - OSI networking and system aspects - Abstract Syntax Notation One (ASN.1). Information technology - Abstract Syntax Notation One (ASN.1): parametrization of ASN.1 specifications".

[20] ITU-T Recommendation X.751 (1995): "Data networks and open system communication - OSI management. Information technology - Open Systems Interconnection - Structure of management information: Change over function".

[21] ITU-T Recommendation X.721 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Structure of management information: definition of management information".

[22] ITU-T Recommendation X.746 (1995): "Data networks and open system communication - OSI management. Information technology - Open Systems Interconnection - Structure of management information: Scheduling function".

[23] ITU-T Recommendation X.725 (1995): "Data networks and open system communication - OSI management. Information technology - Open Systems Interconnection - Structure of management information: General relationship model".

[24] ITU-T Recommendation X.730 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Systems Management: Object management function".

[25] ITU-T Recommendation X.731 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Systems Management: State management function".

[26] ITU-T Recommendation X.732 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Structure of management information: Attributes for representing relationship".

[27] ITU-T Recommendation X.733 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Structure of management information: Alarm reporting function".

[28] ITU-T Recommendation X.734 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Structure of management information: Event report management function".

[29] ITU-T Recommendation X.735 (1992): "Data communication networks. Information technology - Open Systems Interconnection - Structure of management information: Log control function".

[30] ITU-T Recommendation X.737 (1995): "Data communication networks. Information technology - Open Systems Interconnection - Structure of management information: Confidence and diagnostic test categories".

[31] ITU-T Recommendation X.738 (1993): "Data networks and open system communication - OSI management. Information technology - Open Systems Interconnection - Structure of management information: Summarization function".

[32] ITU-T Recommendation X.745 (1993): "Data networks and open system communication - OSI management. Information technology - Open Systems Interconnection - Structure of management information: Test management function".

3 Definitions and abbreviations

3.1 Definitions

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

alarm event: an instantaneous occurrence that changes at least one of the attributes of the alarm status of an object. This status change may be persistent or temporary, thus allowing for surveillance, monitoring, performance measurement functionality, etc. Alarm events may or may not generate alarm reports; they may trigger other events or may be triggered by one or more other events (ITU-T Recommendation Q.821 [14]).

alarm report: a specific type of event report used to convey alarm information (ITU-T Recommendation X.733 [27]).

alarm status: a set of attributes that describes the alarms currently defined for an object, for example, Perceived Severity. The alarm status of an object is a subset of the global status of that object (ITU-T Recommendation Q.821 [14]).

alarm surveillance: a set of functions that enables the monitoring or interrogation (or both) of the telecommunications network concerning alarm-related events or conditions (ITU-T Recommendation Q.821 [14]).

alarm: a specific type of notification concerning detected faults or abnormal conditions (ITU-T Recommendation X.733 [27]).

NOTE: This definition is taken from chapter 7 of ITU-T Recommendation X.733 [27]. The same document has a different definition in chapter 3 which is not adopted in the scope of the present document.

back-up: a back-up relationship is an asymmetric relationship denoting that the second of a pair of managed objects (the back-up object) is currently active and performing a back-up function in place of the first (the backed-up object) (ITU-T Recommendation X.732 [26]).

cold standby: a secondary resource that requires initialization activity before it can provide back-up capability is defined as being in a cold standby state (ITU-T Recommendation X.751 [20]).

event: an instantaneous occurrence that changes at least one of the attributes of the global status of an object. This status change may be persistent or temporary, thus allowing for surveillance, monitoring, and performance measurement functionality, etc. Events may or may not generate reports; they may be spontaneous or planned; they may trigger other events or may be triggered by one or more other events (ITU-T Recommendation Q.821 [14]).

fallback: a fallback relationship is an asymmetric relationship denoting that the second of a pair of managed objects (the secondary object) is capable of serving as a fallback or "next preferred choice" to the first managed object (the primary object) (ITU-T Recommendation X.732 [26]).

global status: the complete set of attributes necessary to describe an object at a particular time (ITU-T Recommendation Q.821 [14]).

hot standby: a secondary resource that is able to provide back-up capability for a primary resource, without the need for initialization activity is defined as being in a hot standby state (ITU-T Recommendation X.751 [20]).

installation: installation is the operation concerning the placement of resources at a required position, as well as, the physical interconnection of the network and the supporting elements and their components. It is also responsible for the replacement or removal (decommissioning) of equipment or the extension of existing equipment. Installation includes the physical intervention on the resource (which is out of the scope of the present document) and the electronic management of the first initialization of a physical resource previous to its actual provisioning.

protection (or redundancy): the capability of a system to perform fault tolerant functionality by means of spare resources (or groups of resources) (EN 301 251 [1]).

provisioning: provisioning consists of procedures which are necessary to bring an equipment into service, not including installation (ITU-T Recommendation M.3400 [8]).

3.2 Abbreviations

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

AO	Associated Object
ASN.1	Abstract Syntax Notation One
CMIS	Common Management Information Service
EFD	Event Forwarding Discriminator
GFM	General Functional Model
GSM	Global System for Mobile Communications
RU	Replaceable Unit
MF	Mediation Function
MIB	Management Information Base
MORT	Managed Object Referring to Test
NE	Network Element
NEF	Network Element Function
NEML	Network Element Management Layer
NEL	Network Element Layer
OS	Operations System
OSF	Operations System Function
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PRM	Physical Resource Management
PT	Pass Through
SDH	Synchronous Digital Hierarchy
SMAP	Systems Management Application Protocol
STC	Sub-Technical Committee
TM	Transmission and Multiplexing
TMN	Telecommunications Management Network
TO	Test Object

4 Telecommunications Management Network (TMN) management context

4.1 Level of abstraction

There are several different viewpoints of management information which may be defined for management purposes, with the Network Element (NE) level viewpoint, the Network level viewpoint and the Service level viewpoint defined below. These viewpoints are not restrictive but define the levels of abstraction of particular types of interfaces. That is, object class definitions are not forced into this categorization but are constructed to meet the needs of exchanging management information across TMN interfaces. Objects defined for a given viewpoint may be used in others, and any object may be used by any interface which requires it. The definition of viewpoint is a means of generating requirements, hence there is no implicit definition of interfaces or storage requirements. This information is defined for the purpose of management via an open interface.

The NE level viewpoint is concerned with the information that is required to manage a NE. This refers to the information required to manage the Network Element Function (NEF) and the physical aspects of the NE. The information may be derived from open systems other than the NE.

The Network level viewpoint is concerned with the information representing the network, both physically and logically. It is concerned with how network element entities are related, topographically interconnected, and configured to provide and maintain end-to-end connectivity.

The Service level viewpoint is concerned with how network level aspects (such as an end-to-end path) are utilized to provide a network service, and as such is concerned with the requirements of a network service (e.g. availability, cost, etc.) and how these requirements are met through the use of the network, and all related customer information.

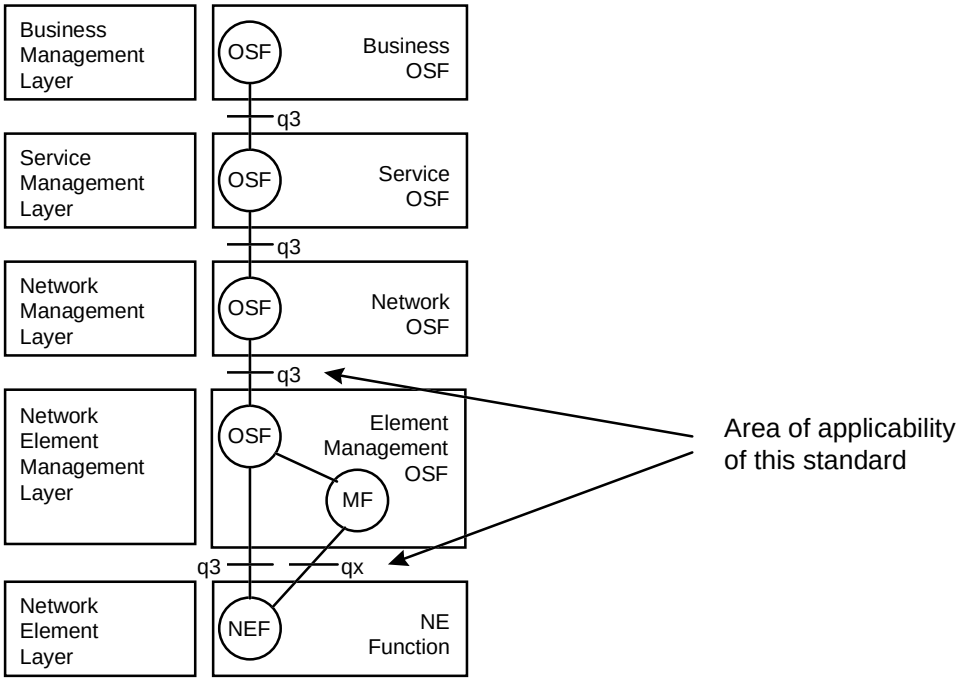

Figure 1: TMN OS functional hierarchy

The present document relates to the management of physical resources and does not specify objects relating to a single interface. Physical resource management functionalities may be split between the element OSF and the network OSF and the management of physical resources may be applicable at both the Network Layer OS to Network Element Layer OS interface (e.g. for network level inventory management) and Network Element Layer (NEL) OS to the Network Element interfaces (e.g. for network element fault and configuration management).

4.2 Management view

The present document covers the configuration management and the fault management functional areas, including testing, timing, protection and inventory. Within each management views, the standard addresses the management of physical resources (hardware) comprising a network element. This includes the peripheral/accessories parts subject to management action (e.g. disk, power supply, fan equipment etc.).

Configuration management functional area: the generic configuration features of the physical and administrative resources pertaining to the physical resource management are considered. This includes the management of timing subsystems and interfaces to external timing generators, the management of physical resources in order to provide protection mechanisms and the management of the inventory information pertaining to the physical resources.

Fault management functional area: the generic fault management features of the physical and administrative resources pertaining to the physical resource management are considered. This includes fault management features defined in ITU-T Recommendation Q.821 [14] and ITU-T Recommendation X.733 [27] and pertaining to physical resources, the generic testing of physical resources according to ITU-T Recommendation X.745 [32] and the management of protection operations as a consequence of faults.

The present document does not cover the performance management functional area as requirements and management functions in this area are usually treated at higher logical levels of abstraction (e.g. definition of thresholds, performance monitoring, etc.) than that of hardware resources.

4.3 Resources

This subclause describes the physical and administrative resources that shall be managed within the scope of the present document.

The mapping of physical resources to managed object classes is provided in subclause 5.1.1.

Figures 2 to 5 are examples of physical resources organization within a NE. These examples are just a simple representation of the actual physical resource positioning in a NE and are not meant to be exhaustive nor complete. The intention is to give a general view of the situation. Real situations usually deal with very complex configurations (e.g. cables connected to multiple connectors, slots containing two half size cards, subracks that do not use back panels, etc.).

Figure 2 shows the relationship existing between rows, racks and subracks.

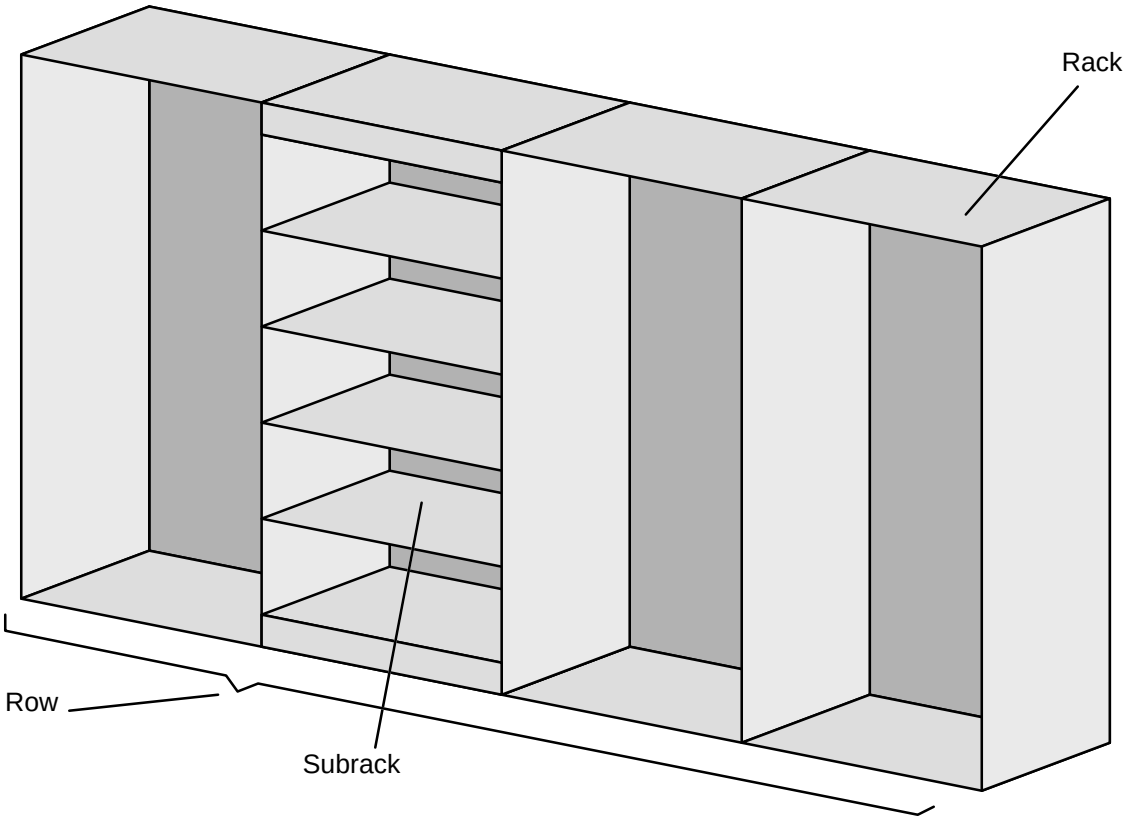

Figure 2: A possible row, rack, subrack organization.

Figures 3 and 4 show a typical organization of physical resources within a NE. A subrack contains slots which contain cards. The back panel is an additional item contained by the subrack that may contain circuitry. Connectors are placed onto the back panel and cables are plugged into the connectors. The relationship between internal and external connectors (figure 4) may depend on the back panel structure.

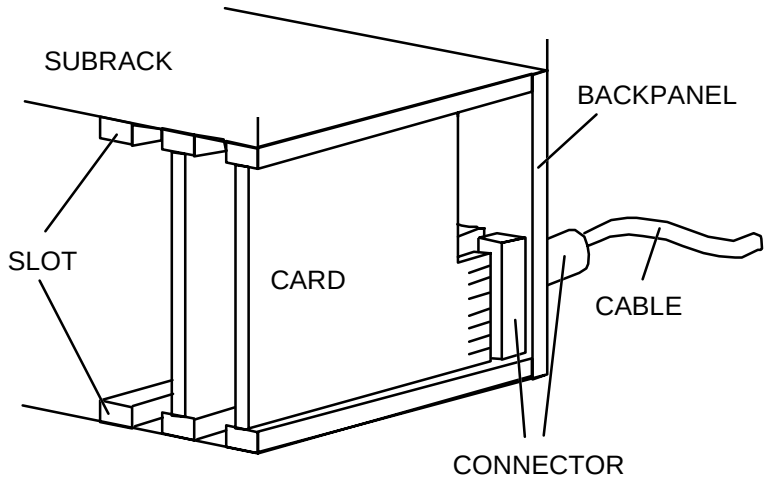

Figure 3: A possible physical resource organization (perspective view)

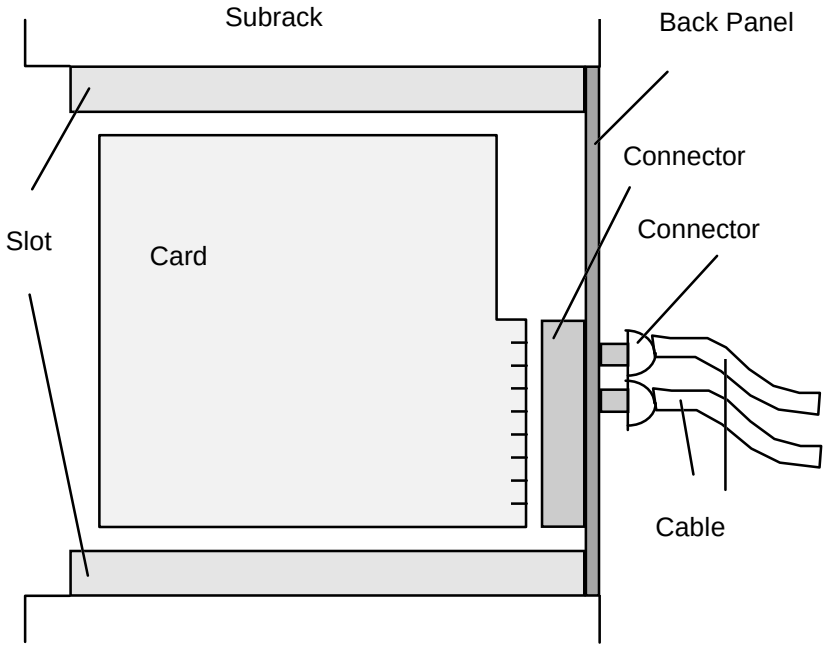

Figure 4: A possible physical resource organization (side view)

An example of the physical connectivity relationship between physical resources is illustrated in figure 5, where a cable connects two connectors.

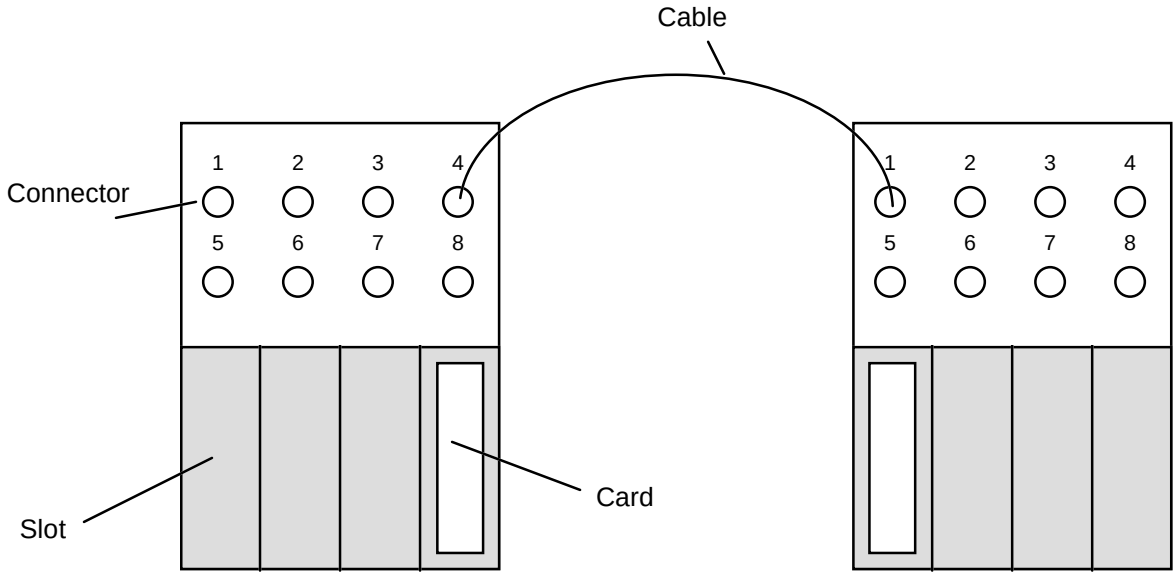

Figure 5 - Example of physical connectivity.

4.3.1 Row

A row comprises one or more racks. The grouping is vendor and/or customer dependent according to several criteria (e.g. power consumption, encumbrance). This resource enables the location of individual physical entities to be identified.

NOTE: Another term used to describe this resource is suite.

4.3.2 Rack

A rack is a free-standing or fixed structure for housing of electrical and/or electronic equipment. (ETS 300 119-1 to 4 [2] to [5]).

The rack represents the basic holder of physical resources. It has specific properties depending from several factors (e.g. manufacturer, technology, dimensioning) that affect the contained physical entities. Usually the rack is considered (and managed) as a matrix of equipment locations for example subracks and cards. This resource enables the location of individual physical entities to be identified.

NOTE: Other terms used to describe this resource are bay and cabinet.

A cabinet is a free-standing and self-supporting enclosure for housing electrical and/or electronic equipment. It is usually fitted with doors and/or side panels which may or may not be removable. (ETS 300 119-1 to 4 [2] to [5]).

4.3.3 Subrack

Subracks are used in miscellaneous racks/cabinets. The subrack will normally be supplied as a fully assembled structure, unequipped, partially equipped or fully equipped with plug-in units, etc. (ETS 300 119-1 to 4 [2] to [5]).

One or more subracks representing the rows in the matrix representation are contained in a rack. The subrack may introduce additional restrictions on the allocable location characteristics. For example a power supply subrack could only accept a power supply. This resource enables the location of individual physical entities to be identified.

NOTE: Another term used to describe this resource is shelf.

4.3.4 Slot

The slot is the most elementary holder of equipment. In the matrix representation it represents the cell element.

This resource is characterized by essentially three factors: physical (i.e. dimension), electrical and connection (in case of a fixed back panel connector).

4.3.5 Card

The card represents a plug in element (e.g. field replaceable unit) within the slot. There exists a relationship between a card and the usable slots.

4.3.6 Back panel

This is a specific type of non replaceable card that contains connectors which are associated with plug in elements and cables. Typically there is one back panel per subrack. A back panel may support functionalities that are manageable.

4.3.7 Storage device

The storage device is a depository of files (that is collections of structured information). The storage device contains, for example, the source which is used for reference to create another instance of software unit in a target equipment subclass.

4.3.8 Power supply

This entity describes the resources used to provide power to the NE entities. There could be several specializations of this entity describing specific resource peculiarities.

4.3.9 Connector

Associated with each slot or card there could exist one or more connectors which represents the physical access points to contained cards (if any). Several connector types exist to support different connections (e.g. power, data transmission).

4.3.10 Cable

The cable is the passive resource providing physical connection between connectors. The cable could also be represented by the back plane in which case the association between cable and connector is fixed during production.

4.3.11 Module

This resource represents a relationship between several physical entities for administrative purposes.

4.3.12 Audio or visual indicator

This applies to resources such as bells and lamps.

4.3.13 Physical group

A NE may have for administrative reasons one or more physical groups which comprise one or more racks at a single location.

4.3.14 Timing generator

The timing generator produces the clock signals within a NE.

4.3.15 Timing receptor

The timing receptor is a physical resource in charge of interfacing to an external timing generator and distributing the clock signals internally within the network element.

4.3.16 Sensor interface unit

This is the physical resource (e.g. environmental sensor, door switch) responsible for interfacing to systems external to the network element and not pertaining to telecommunications systems.

4.4 Applicable requirements

This subclause contains a collection of all the applicable requirements for physical resource management. The following requirements have been extracted from (ITU-T Recommendation M.3400 [8]) and a number of other related Recommendations. The requirements relating to physical resources are restricted to fault and configuration management areas.

It should be noted that not all of the requirements can be supported by the current version of the object model.

4.4.1 Fault management

4.4.1.1 Alarm Surveillance (EN 301 251 [1])

Alarm surveillance requires that the OS and the operator have a consistent and up-to-date view of the current operating condition and quality of service of the managed network element. For efficient and accurate fault management of a network it is also essential to achieve early detection of faults so that they can be corrected before significant effects have been felt by the end-user.

This results in the following requirements:

1) It is required that all detected faults and anomalies in the NE are reported to the OS (for each case which matches the reporting conditions set by the OS). The NE/OS shall therefore support the sending/reception of unsolicited event reports notifying such events.

NOTE: The definition of detection functions (e.g. threshold management for quality of service alarms) is out of the scope of the present document.

2) The forwarding of alarm reports through the Q3 interface shall be manageable both in terms of filteringalarm reporting is based on the model described in ITU-T Recommendation X.734 [28], that is: the result of the fault detection process shall be an alarm notification sent to the event pre-processing which may generate a potential event report that is sent to all the existing Event Forwarding Discriminators (EFDs). The EFD is a managed object which receives the potential alarm reports and determines which event reports are to be forwarded and which are to be discarded. For the forwarded reports it also determines the destination, the time frame and the forwarding mode (confirmed or non-confirmed). The correlation and filtering of potential alarm reports can be used for example to identify the original cause of an alarm event and to group under a unique notification, data pertaining to multiple notifications related to the same event.

3) The NE shall be able to log alarm information as alarm records and support later retrieval of the logged alarm records. The logging functionality is based on the model described in ITU-T Recommendation X.735 [29] and can be used for any type of event information, including the alarm information. According to this model, when a fault is detected, an alarm notification is also sent to the log pre-processing which may generate a potential log report that is sent to all the existing logs. The log is a managed object which receives the potential log reports and determines which of them are stored as log records and which are discarded.

4) The NE shall be able to provide information to the OS about all the current outstanding alarm conditions in the NE. The outstanding alarm information may be reported in a summary, on demand or periodically to the OS. This functionality is based on ITU-T Recommendation Q.821 [14] and can be used to have a view of NEs current alarm condition from the NE on demand at any time. This functionality can also be used to align alarm information between the OS and NE for instance after an interruption of communication between the OS-NE (e.g. link failure, OS restart, NE restart) without waiting for the forwarding of all the events which occurred during the failure.

To support these alarm surveillance requirements over the Q3 interface, a number of management functions are foreseen and defined in more detail in subclause 4.5.1.1. These functions are grouped as follows:

- Alarm reporting (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14], ITU-T Recommendation X.733 [27], ITU-T Recommendation X.734 [28])
- Alarm summary (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14])
- Alarm event criteria (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14], ITU-T Recommendation X.733 [27])
- Alarm indication management (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14])
- Log control (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14], ITU-T Recommendation X.735 [29])
- Alarm correlation and filtering (ITU-T Recommendation M.3400 [8])

4.4.1.2 Fault localization

Fault localization shall provide all the necessary information in order to localize the faults that may occur in the NE. The main requirements are as follows:

1) The NE shall be able to execute diagnostic tests in order to localize the fault when the alarm notification generated was not sufficient to identify the cause of the fault (the execution may be automatic or requested by the OS). The result of diagnostic tests shall be reported to the OS and the execution may be scheduled according to routine criteria. Ongoing diagnostic tests may be stopped, if required, by the OS.

2) The NE shall be able to send to the OS selected log records in order to determine what has occurred in the NE.

3) The NE shall be able to send to the OS any required information on configuration, status and attributes which are relevant to the process of fault localization.

4) The NE may be able to identify the corrective action. This requirement is significant when no information on proposed actions was present in the alarm event notification.

4.4.1.3 Fault correction

Fault correction includes capabilities which are involved when recovery actions are required, that is at fault detection time, after fault repair or on request by the operator. The main requirements are:

1) The NE shall be able to manage equipment protection actions (e.g. hot and cold standby). It is therefore required that the NE be able to invoke or release a protection action and that the results of these actions be reported to the OS.

2) The result of the restoration of a fault shall be reported both in the case of automatic restoration and in the case of OS requested actions.

4.4.1.4 Testing (ITU-T Recommendations X.745 [32] and X.737 [30])

This subclause defines requirements for the remote control of tests and provides a framework for the specification of tests which exercise resources included in an open system. The requirement for the same test functionality may originate from differing higher level areas such as fault or performance management. For example a particular test may be used to generate information that may be of use either in the verification of correct functionality, diagnosis of a fault or in the generation of performance statistics.

A test is the operation and monitoring of open systems, or parts thereof, within an environment designed to elicit information regarding the functionality and/or the performance of the subject system(s).

Each test may involve creating the environment for the test, control and monitoring of the test operation, and reassertion of the normal environment. Control of a test includes the need to suspend, resume and terminate tests. Each test will require a unique identification so that, for example, data generated by the test can be tracked.

In some cases, there is a requirement to specify tests that may be suspended, resumed and terminated when pre-defined conditions are encountered.

Features of the systems environment which may require alteration for testing are:

- the connections to other open systems;
- the configuration of the subject systems;
- the workloads requested of the subject systems.

In some cases, there is a requirement for scheduling tests. The scheduling of tests shall be considered in both a periodic and an aperiodic way. For such tests there is also a requirement to allow modification of the schedule. There is also, in some cases, a requirement for allowing the test to be performed at a time convenient to the system which is to perform the test.

A test may need to be specified such that it becomes active when a preset condition exists (i.e. a threshold is crossed) or when a specific event is detected.

Requirements exist to create more complex tests from simpler ones. For example, to provide the result of many subordinate tests in a single result, or to sequence tests to efficiently diagnose a fault in an entity with a large number of components.

It may be necessary to perform a number of individual tests which together fulfil a specific requirement. In such cases, it is necessary to correlate the results of each test in order to formulate an outcome. There may also be a need for global uniqueness.

This function is seen as being applicable to different test methodologies, for example, loopback tests which configure a resource in such a way that the data sent is then received; fault injection tests in which errors are deliberately introduced in order to verify that such errors are handled properly; or self-tests which simply provide a pass-fail indication.

It may be defined a basic set of confidence and diagnostic test categories that is required by the user of a communication system or network to:

- confirm the ability of a specified part of the system or network to perform correctly its allotted function (that is, the tested entity continues to perform according to its design);
- perform testing, following notification or detection of a fault, to further isolate the cause of the problem.

This requirement includes the need to:

- verify connection between two known end points;
- verify that connectivity may be established between two entities within a specified time;
- verify whether two entities can exchange data without any corruption and measure time taken for the exchange;
- verify that data can be sent and received over a communications path within a specified interval of time;

- determine if two entities can conduct proper protocol interactions;
- verify the observable behaviour of an entity at its boundaries;
- verify the ability of an entity to perform its allotted function;
- verify the ability to receive incoming test requests and generate appropriate responses.

4.4.2 Configuration management

4.4.2.1 Installation

The installation process strongly depends on network operator processes but a set of basic requirements are to be fulfilled to provide control over the installation operations. Installation of resources in the NE may involve physical resources, software resources and logical resources. The order in which all the installation operations are executed is a matter of NE implementation and therefore is out of the scope of the present document. This subclause is concerned with the installation of physical resources.

Installation of physical resources requires that the NE be able to update its database with the newly installed equipment. If installation requires the removal of old physical resources the NE shall also be able to delete the obsolete entries from the database. Newly installed resources may require initial settings of some parameters in order to be tested and subsequently put into service. The NE shall be able to emit notifications for all operations concerning insertion and/or removal of physical resources and for the initialization and/or variation of each resource characterization.

The relevant information that a physical resource shall carry are:

- Valid Physical Possibilities - Identify the different types of equipment that may be inserted into a particular slot;
- Actual Type - Identify the actual type of equipment that is inserted into a slot;
- Actual Instance - Identify the specific instance of a card that is inserted into a slot;
- Valid Administrative Possibilities (Type) - Restrict the possible types of cards that may be inserted.

Installation shall also provide access to undergoing jobs: the operator accessing to the NE shall be able to request a report when the installation is completed and shall be able to request and/or delete existing summaries of installation jobs in the NE.

4.4.2.2 Provisioning

Provisioning consists of procedures which are necessary to bring an equipment into service, not including installation (ITU-T Recommendation M.3400 [8]).

Provisioning requirements for physical resources cover inventory, configuration and protection.

The whole set of physical resources installed in a NE is contained in the inventory. This database contains both resources that are available for service and pre-equipped resources that are installed in the NE but have not been put into service yet. Requirements for inventory management include the capability to request and assign idle resources to a configuration, to remove resources from a configuration, to report the actual assignments of resources, to change state of resources (e.g. in service, out of service, stand-by, reserved) and to give access to resource information and resource assignment. Relevant information may be:

- Equipment Type which also incorporates characteristics of the supported software;
- Serial Number;
- Version Number (this may include revision of version and date of manufacture);
- Vendor.

Configuration of the NE fulfils all requirements on the assignment of resources available in an inventory to specific physical or administrative entities. The NE shall be able to configure resources, report the status of a configuration,

request assigned resources, set parameters on resources for the purpose of configuration, create and delete entities and associate resources to them. Configuration status may be reported to the OS either on demand or on a scheduled basis.

Resources are often configured to provide *back-up capability* to achieve availability goals. A *primary* resource may have one or more designated *secondary* resources, which can provide back-up capability for the primary resource. The back-up capability can be provided, for example, when the primary resource is administratively prohibited from use (i.e. the administrative state is locked) or when it becomes inoperable (i.e. the operational state is disabled). (ITU-T Recommendation X.751 [20]).

The potential to provide back-up capability is represented by the *fallback* relationship. The primary object represents the resource that is to be *backed up*; the secondary object represents the resource that can provide *back-up* capability, (ITU-T Recommendation X.751 [20]).

The fallback relationship may be one-way. A primary object could have an attribute that lists its secondary objects, but the secondary objects need not "point back" to the primary object. Similarly, a secondary object could have an attribute that lists its primary objects, but the primary objects need not point back to the secondary object. In some cases, neither the primary object nor the secondary object may have the knowledge of when back-up capability should be provided. A third object is needed that can be requested to establish the back-up relationship. (ITU-T Recommendation X.751 [20]).

Considering that the existence of a fallback relationship is the precondition for establishing a back-up relationship, the change over relationship is defined as the composition of the fallback and back-up relationships.(ITU-T Recommendation X.751 [20]).

4.4.2.3 Status and control

The NE shall be able to give access to the status of physical resources. The status of a resource may be defined according to ITU-T Recommendation X.731 [25], or may be specific for the resource. NE shall be able to report the status of a physical resource either on demand or on a scheduled basis. Spontaneous notifications of changes in the status of a resource shall also be supported. The forwarding of notifications to the OS may be filtered.

4.5 Management Functions

This subclause contains, according to ITU-T Recommendation M.3400 [8], the definition of general functional models and TMN management functions for each of the two TMN functional areas covered by the present document. Functional areas are divided into functional sets, in order to create homogeneous groups of management functions. When available each general functional model and each management function has a direct reference to the normative reference that defines it.

It should be noted that not all of the management functions can be supported by the current version of the object model.

Each management function within a management function set is mapped onto resources in order to have knowledge of which management function is applicable to which resource. Table 1 shows resource groupings that are used for the mapping: each management function is marked with one or more of the defined identifiers.

It shall be noted that physical resources may be divided into active and passive resources. Active physical resources feature functionalities that need to be managed, or are able to emit notifications either spontaneously or on demand. Passive physical resources cannot be managed and usually their presence is embedded in some active resource by means of configuration or inventory data. Examples of passive resources are cables and connectors. In table 1 the back panel is assumed to be an active resource as this physical resource may have built-in functionalities that allow, for example, testing or alarm surveillance. When the back panel is passive (i.e. no built-in intelligence) it is assumed that it is an integral part of an equipment holder (e.g. rack, subrack).

Table 1: Resource grouping for management functions mapping

Identifier	Resource Grouping
A	Rack, Subrack, Row, Slot
B	Card, Back panel, Storage Device, Power Supply
C	Connector, Cable
D	Audio or visual indicator
E	Module, Physical group
F	Sensor interface unit
G	Timing generator, Timing receptor
H	Support resources

NOTE 1: Support resources (H) is used to map management functions on logical resources that are not defined within the present document. Examples are Event Forwarding Discriminators, Logs, Alarm Log Records, etc.

NOTE 2: In the following text, all the letters indicated in bracket refer to table 1.

4.5.1 Fault management

4.5.1.1 Alarm surveillance

Alarm surveillance for the management of physical resources includes the following management function sets:

- Alarm reporting function set (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14], ITU-T Recommendation X.733 [27], ITU-T Recommendation X.734 [28]);
- Alarm summary function set (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]);
- Alarm event criteria function set (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14], ITU-T Recommendation X.733 [27]);
- Alarm indication management function set (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]);
- Log control function set (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14], ITU-T Recommendation X.735 [29]);
- Alarm correlation and filtering function set (ITU-T Recommendation M.3400 [8]).

4.5.1.1.1 Alarm reporting

4.5.1.1.1.1 General Functional Model (ITU-T Recommendation M.3400 [8])

Alarms are specific types of notifications concerning detected faults or abnormal conditions. An alarm notification results from an alarm condition which persists long enough to qualify as a non-transient condition as determined by some algorithm applied to the condition. Such an algorithm may be simple (e.g. "all occurrences of the condition shall be treated as alarms") or complex (e.g. by applying one of the defined threshold types to the condition). When an alarm condition exists, the affected managed object has an "ACTIVE-REPORTABLE" alarm status.

Similarly, when the alarm condition ceases to exist, an alarm notification is generated to report clearing of the alarm. The affected managed objects alarm status is "CLEARED".

When some condition has been recognized but has not persisted long enough to qualify as a non-transient condition (as determined by some algorithm applied to the condition), the affected managed objects alarm status becomes "ACTIVE-PENDING". In the case of a "null" algorithm (i.e. all occurrences of the condition are treated as non-transient), or when the transient conditions can occur too frequently to be meaningfully monitored, the "ACTIVE-PENDING" status will not exist.

Figure 6 illustrates the states and transitions related to the alarm status of managed objects.

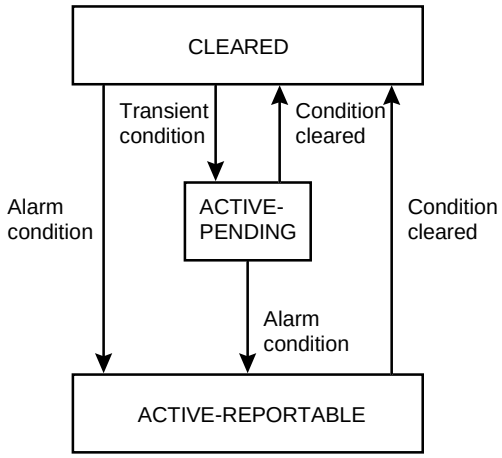

Figure 6: Status and transitions related to the alarm status of managed objects (ITU-T Recommendation [8] 1/M.3400]

An NE shall provide a mechanism for the control of notification, e.g. whether an alarm condition results in an alarm report to the TMN. The requirements to be satisfied are:

- the definition of a flexible alarm report control mechanism which will allow systems to select which alarm reports are to be sent to the TMN;
- specification of the destination to which the alarm reports are to be sent;
- specification of a mechanism to control the forwarding of alarm reports, for example, by suspending and resuming their forwarding;
- the ability for the TMN to modify the conditions used in the reporting of alarm conditions.

4.5.1.1.1.2 TMN Management Functions

1) **Report Alarm** – Agent notifies Manager of alarm information upon the occurrence of an alarm: (B,E,F,G) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

2) **Route Alarm Report** – Manager specifies to the Agent the destination address(es) for a specified set of alarm reports: (H) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

3) **Request Alarm Report Route** – Manager requests Agent to send the current assignment of the destination address(es) for a specified set of alarm reports; Agent responds with the current assignment of destination address(es): (H) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

4) **Condition Alarm Reporting** – Manager instructs the Agent to assign Event Forwarding Discriminator attributes as specified by the Manager: (H) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

5) **Request Alarm Report Control Condition** – Manager requests Agent to send the current assignment of specified Event Forwarding Discriminator attributes; Agent responds with the current assignment of the specified attributes: (H) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

6) **Allow/Inhibit Alarm Reporting** – Manager instructs the Agent to allow/inhibit alarm reports to the Manager: (H) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

7) **Request Alarm Report History** – Manager requests the Agent to send specified alarm information history; Agent responds with the specified information: (H) (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14]).

8) **Delete Alarm Report History** - Manager requests the Agent to delete specified historical alarm information: (H) (ITU-T Recommendation Q.821 [14]).

4.5.1.1.2 Alarm summary

4.5.1.1.2.1 General Functional Model (ITU-T Recommendation M.3400 [8])

The model for current alarm summary reporting describes the conceptual components that provide for the collation of current alarms into a current alarm summary report. The alarms are received from specified managed objects and satisfy defined conditions. The reporting may be on a scheduled or on-demand basis.

The current alarm summary control is used to provide the current alarm summary report for the specified managed objects and condition. It is provided in response to a message from the management operation scheduler or a specific request from the TMN to retrieve the current alarm summary report.

Figure 7 is a schematic representation of the components involved in generating, and reporting current alarm summary reports.

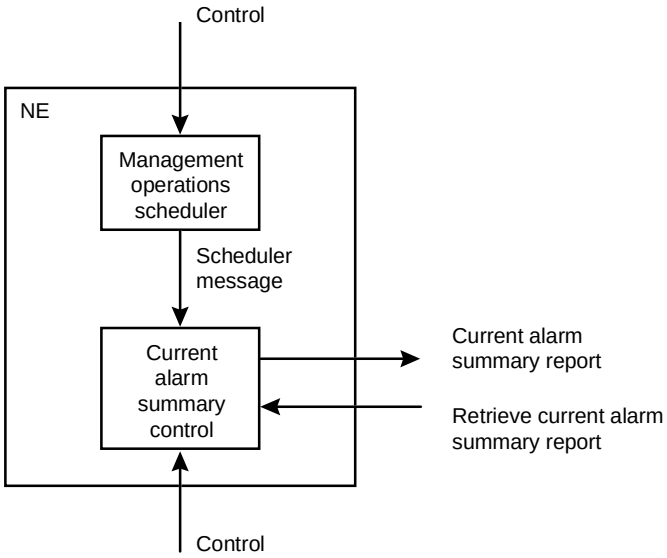

Figure 7: Current alarm summary report (2/M.3400)

4.5.1.1.2.2 TMN Management Functions (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14])

1) **Report Current Alarm Summary** – Agent provides Manager (based on a pre-defined schedule) with a Current Alarm Summary: (H).

2) **Route Current Alarm Summary** – Manager specifies to the Agent the destination address(es) for a specified set of Current Alarm Summaries: (H).

3) **Request Current Alarm Summary Route** – Manager requests Agent to send the current assignment of the destination address(es) for a specified set of Current Alarm Summaries; Agent responds with the current assignment of destination address(es): (H).

4) **Schedule Current Alarm Summary** – Manager specifies a schedule for the Agent to establish for the reporting of Current Alarm Summaries. The schedule information specifies what should be reported as well as when it should be reported: (H)..

5) **Request Current Alarm Summary Schedule** – Manager requests Agent to send the current schedule information for Current Alarm Summary reporting; Agent responds with the schedule information: (H)

6) **Allow/Inhibit Current Alarm Summary** – Manager instructs the Agent to allow/inhibit reporting of the scheduled Current Alarm Summaries: (H).

7) **Request Current Alarm Summary** – Manager requests the Agent to send a Current Alarm Summary; Agent responds with the summary. This function allows a Agent to report alarm conditions of specified resources (severity, status, cause, etc.): (H).

4.5.1.1.3 Alarm event criteria

4.5.1.1.3.1 General Functional Model

The Alarm event criteria functions allow for the assignment of specified attributes used by the NE to determine if a condition is to be considered an alarm. (ITU-T Recommendation M.3400 [8]).

The Alarm event criteria functions allow to control the alarm generation behaviour of managed objects modelling underlying resources within a NE, through modifying specified attributes. Conditions are thus determined under which a notification shall be emitted from a managed object modelling an underlying resource.

NOTE: The examples relating to thresholds have been omitted as alarm event criteria provides only for alarm severity assignment (ITU-T Recommendation Q.821 [14]). The setting of threshold related attributes is in the scope of performance management. Alarm event reports may contain threshold information when the alarm is the result of a threshold crossing as stated in ITU-T Recommendation X.733 [27].

4.5.1.1.3.2 TMN Management Functions (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14])

1) **Condition Alarm Event Criteria** – Manager instructs the Agent to assign specified alarm attributes (e.g. thresholds, etc.) used by the Agent to determine if an event is to be considered an alarm: (H).

2) **Request Alarm Event Criteria** – Manager requests Agent to report the current assignments of specified attributes (e.g. thresholds, etc.) used to determine if an event is to be considered an alarm; Agent responds with the current assignment of the requested attributes, modes, or thresholds: (H).

4.5.1.1.4 Alarm indication management

4.5.1.1.4.1 General Functional Model (ITU-T Recommendation M.3400 [8])

The alarm indication management function set allows to control audible/visible indications.

4.5.1.1.4.2 TMN Management Functions (ITU-T Recommendation M.3400 [8], ITU-T Recommendation Q.821 [14])

1) **Inhibit/Allow Audible/Visual Alarm Indications** – Manager instructs the Agent to inhibit/allow the operation of specified alarm indication/recording devices such as lamps, speakers, printers, etc. In the inhibit mode, new alarms will not trigger audible/visual alarm indicators: (A,B,E,F,G).

2) **Reset Audible Alarms** – Manager instructs the Agent to reset specified audible alarm indicator(s). This function momentarily removes any alarm indications, but allows further alarms to trigger audible/visual indicators: (A,B,E,F,G).

4.5.1.1.5 Log control

4.5.1.1.5.1 General Functional Model

For the purpose of alarm surveillance, it is necessary to preserve information about alarm reports that have occurred as a result of alarm reports on managed objects. Alarm records in the log contain the information from their corresponding alarm reports, (ITU-T Recommendation M.3400 [8]).

The model for the log control functions describes the conceptual components that provide for the logging and retrieval of alarm information. Figure 8 is a schematic description of the alarm logging capability.
(ITU-T Recommendation M.3400 [8]).

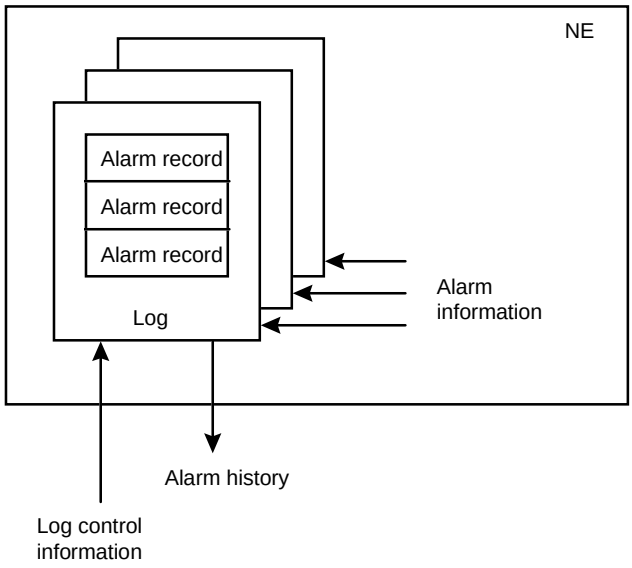

Figure 8: Alarm logging capability (3/M.3400)

It is considered that a manager should have the capability of modifying the operation of a log in a remote system (ITU-T Recommendation X.735 [29]). In particular, the operations required, that can be applied to each instance of a log, are:

- creation of a log;
- deletion of a log;
- deletion and retrieval of log records.

4.5.1.1.5.2 TMN Management Functions

1) **Allow/Inhibit Logging** – Manager instructs the Agent to allow/inhibit logging of log records: (H) (ITU-T Recommendation Q.821 [14], ITU-T Recommendation M.3400 [8]).

2) **Condition Logging** – Manager instructs the Agent to assign Log attributes as specified by the Manager: (H) (ITU-T Recommendation Q.821 [14], ITU-T Recommendation M.3400 [8]).

3) **Request Log Condition** – Manager requests Agent to send the current assignment of specified log attributes; Agent responds with the current assignment of the specified attributes: (H) (ITU-T Recommendation Q.821 [14], ITU-T Recommendation M.3400 [8]).

4) **Create/Delete log** - Manager requests Agent to create/delete a log; Agent creates/deletes the requested log: (H) (ITU-T Recommendation X.735 [29]).

5) **Retrieve log records** - Manager requests Agent to send log records from a log; Agent responds by sending the requested log records: (H) (ITU-T Recommendation X.735 [29]).

6) **Delete log records** - Manager requests Agent to delete log records from a log; Agent deletes the requested log records: (H) (ITU-T Recommendation X.735 [29]).

4.5.1.1.6 Alarm correlation and filtering

4.5.1.1.6.1 General Functional Model (ITU-T Recommendation M.3400 [8])

Correlation involves interpreting state changes which occur in networks, network elements, and operational equipment or systems, in the light of related conditions and circumstances. A state change may be meaningful of itself, or only when specific other state changes occur, possibly in a predefined time-order, or when specific other state changes do not occur.

State changes are normally manifested as events or notifications which are emitted spontaneously by the equipment or system where the state change occurred.

Events which are transient, redundant, implied or fit into a known pattern can be correlated, with only the interesting "master" root cause events presented to a network operator.

Events should be processed as close to their source as possible and immediately upon their arrival at the management system.

4.5.1.1.6.2 TMN Management Functions (ITU-T Recommendation M.3400 [8])

1) **Determine identity of event** - Agent provides Manager with events unique identity: (H).

2) **Filter events** - Manager requests Agent to select specific event(s) from a general stream of events: (H).

NOTE: This filtering differs from the event forwarding discriminator which is used only to determine which event reports are to be forwarded to a particular destination during specified time periods. The TMN management function of "Filter events" can eliminate, that is, filter any user defined set of conditions.

3) **Suppress transient events** - Manager requests Agent to suppress events which only occur on a rare and intermittent basis which are not of consequence to the network services: (H).

4) **Suppress redundant events** - Manager requests Agent to suppress redundant events, but count those events: (H).

5) **Suppress implied events** - Manager request Agent to suppress all events which are implied by root cause event, but enhance information in root cause event: (H).

6) **Maintain event inter-dependencies** - Manager requests Agent to evaluate significance of event based on one or more other events which are generated and delivered independently: (H).

7) **Handle event arriving out of order** - Manager handles events received from Agent, which due to different network transient delays or clock skew in the device and manager systems, arrive in a different order than their creation time order: (H)

8) **Handle environmental conditions** - Manager requests Agent to correlate events based on environmental conditions such as business rules, time of day, configuration values, affecting event significance: (H).

9) **Access external data sources** - Manager requests Agent to correlate events based on information stored externally: (H).

10) **Trigger automatic action** - Manager requests Agent to initiate an action to be taken based on event information: (H).

11) **Take action which is based on non-arrival of an event** - Manager requests Agent to wait for the receipt of an event, and in turn initiates an action based on the non-arrival of the event within a specified period of time: (H).

12) **Receive raw data***:* Manager receives alarm and other events from Agent: (H).

13) **Root cause message***:* Manager receives root cause notification from Agent: (H).

14) **Forward alarms***:* Manager receives analysed, filtered alarms and other events from Agent: (H).

4.5.1.2 Fault localization

4.5.1.2.1 General Functional Model (EN 301 251 [1])

Fault localization requires that the NE has the capability to provide all the necessary information to the OS in order to localize the faults that may occur in the NE itself.

In the process of localizing the faults, the first information is provided by the alarm surveillance service component, since after the fault detection an alarm notification is generated and, if the corresponding potential report is not discriminated, an alarm report which should contain sufficient information to localize the fault is forwarded to the OS.

Whenever possible, the NE should generate a single notification for a single fault. When a single fault results in the failure of other functionalities, the system should filter these "dependency faults".

In case of ambiguity in the localization, the operator can require, from the NE:

- the execution of diagnostic tests;
- retrieval of some log-records to have a clear view of the events that occurred before the failure;
- other information like the current configuration, the value of some measurements, the value of some attributes, etc.

Testing may also be needed to verify the fault if the localization process is initiated due to, for instance, customer complaints instead of an alarm report.

The detailed fault localization process is a matter of the NEs internal architecture as well as operators maintenance and operating procedures and thus not a subject for standardization.

The resolution of the localization should be down to one Replaceable Unit (RU - single resources to be replaced - e.g. card) for the majority of the faults. When the NE cannot localize the fault to one RU, it should indicate a restricted number of RUs, ordered according to the probability of being faulty.

4.5.1.2.2 TMN Management Functions

Fault localization makes use of TMN management functions defined in subclause 4.5.1.1 subclause 4.5.1.4 and subclause 4.5.2.3 of the present document.

4.5.1.3 Fault correction

4.5.1.3.1 General Functional Model (EN 301 251 [1])

Fault correction requires capabilities that are used in different phases of the fault management:

1) Right after a fault detection, the NE shall be able to evaluate the effect of the fault on the telecommunications services and autonomously make all the recovery actions in order to minimize the effect of the fault on the services provided to the users.

2) Once the fault has been repaired, it shall be possible from the OS, to put the repaired resources back to service so that the NE is restored to its optimal working configuration. This transition shall be done in such a way that the currently provided telecommunications services are not (or minimally) disturbed.

3) At any time the NE shall be able to perform recovery actions if requested by the operator. The operator may have several reasons to require such actions; e.g. he has deduced a faulty condition by analysing and correlating alarm reports, or, merely, he wants to verify that the NE is capable of performing the recovery actions (pro-active maintenance).

The recovery actions that the NE shall perform (autonomously or on demand) in case of fault depend on the nature and severity of the faults, on the hardware and software capabilities of the NE and on the current configuration of the NE.

In the case of hardware faults, the recovery actions depend on the existence and type of redundant (back-up) resources.

If the faulty resource has no redundancy, the recovery actions are:

a) isolate and remove from service the faulty resource so that it cannot disturb other working resources;

b) remove from service the physical and functional resources (if any) which are dependent on the faulty one. This to prevent the propagation of the fault effects to other fault-free resources;

c) adjust the Operational State and Status attributes of the faulty managed object and the affected managed objects, in a consistent way, reflecting the new situation;

d) generate and forward (if possible) the reports to inform the OS about all the changes performed.

If the faulty resource has redundancy, the NE shall perform actions a), c) and d) above and, in addition, the recovery sequence which is specific to that type of redundancy.

In the NE the redundancy of some resources may be provided to achieve the fault tolerance and to improve the system availability. There exist a lot of types of redundancy (e.g. hot standby, cold standby, duplex symmetric/asymmetric, N plus one or N plus K redundancy, etc.) and for each one, in case of failure, there is a specific sequence of actions to be performed. The present document is concerned with the management of (how to monitor and to control) the redundancies, but does not define the specific recovery sequences of the redundancy types.

The redundancy behaviour describes how the redundancy works (when and how the change-over takes place) and how the redundancy is managed (how the operator can know the current active/standby object, how the operator can trigger a change-over for preventive maintenance, etc.).

The management of the redundancies is strictly related to the way they are modelled in the Management Information Base (MIB) of the NE. For the modelling of the redundancies, the relationships shall be defined among the objects which participate in each redundancy. This shall identify the objects and the roles that they have in the redundancy. By defining the relationships, also the roles of the objects participating to the relationships are implicitly defined by the relationships attribute values.

The NE shall provide the OS with the capability to monitor and control any redundancy of the NE. The control of a redundancy (which, in this case, means the capability to trigger a change-over or a change-back) from the OS can be performed by means of the state management services or by means of specific actions.

When the state management services are used, the transitions are triggered by locking/unlocking one of the objects participating to the redundancy. In this case, for the management of the redundancy, the locking and unlocking should be processed, by the NE, with the same logic of disabling/enabling, triggered by the fault-detection/fault-correction.

In the case of a failure on a resource represented by the providing service managed object, the recovery sequence shall start immediately, and before or during the change-over, a temporary and limited loss of service (if any) shall be accepted. Conversely in the case of a management command, the NE should perform the change-over without degradation of the telecommunications services.

4.5.1.3.2 TMN Management Functions

1) **Change over** - The Manager requests the Agent to provide back-up capability: (B,E,G) (ITU-T Recommendation X.751 [20])

2) **Change back** - The Manager requests the Agent to terminate providing back-up capability: (B,E,G) (ITU-T Recommendation X.751 [20])

3) **State change reporting** - The Agent reports any state change connected to change over. (B,E,G) (ITU-T Recommendation X.751 [20])

4.5.1.4 Testing

4.5.1.4.1 General Functional Model (EN 301 251 [1])

The NE should provide a set of tests which homogeneously cover all the physical and functional parts of the system. Every possible fault occurring on every part of the NE should be covered by at least one test. The tests shall localize the faults as precisely as possible: for the majority of the faults the localization should be on one least replaceable unit.

The NE shall be able to provide to the OS the list of the supported test (both controlled and uncontrolled tests) and all the relative information.

On the NE, the received test requests shall be carefully checked to be sure that the test execution never produces any uncontrolled and undesired effect on the telecommunications services currently provided by the NE itself. These acceptance checks depend on the type of test (intrusive or not intrusive), on the current state of the resources to be tested Managed Object Referring to Tests (MORTs), on the current state of other involved resources necessary to set up the test environment Associated Object (AO), on the current state of the Test Objects (TO), on the availability of the test infrastructures, etc.

The non intrusive tests can be run independently from the state of the MORTs and therefore they do not require any preliminary change of state of the MORTs.

The intrusive tests can be run only if the MORTs are in the "locked" administrative state and/or in the "disabled" operational state. The operator may use the state management services to change the administrative state of the MORTs; the change from unlocked to locked can be graceful, using the transient "shutting down" state.

Depending on the result of the tests, the operational state of the MORTs can change from enabled to disabled if some tests do not pass or, vice versa, from disabled to enabled if all the tests pass. In the first case, when the tests detect a fault, they have to generate an alarm notification using the alarm surveillance service. In the second case when the MORTs are returned enabled they have to generate an alarm notification with "cleared" severity and forward it to the EFD.

It is also possible that some tests fail because of minor faults, so it could be convenient to leave the MORT in service (enabled) instead of removing it from service. In these cases, the availability status "degraded" shall be used to remind that the MORT is not in perfect condition; it is enabled but it has some minor trouble that needs to be corrected.

If the NE provides the capability to execute controlled tests, then it shall be possible, from the OS, to:

- suspend and resume tests;
- monitor the evolution of the tests through the state attribute of the TOs;
- terminate the tests;
- get the results from the TO when they are provided as attributes.

When a controlled test is suspended, the TO is put in the "suspended" state while the involved resources (the AO) may be released or not, depending on the specific characteristics of the TO. When the test is resumed, the TO itself determines at what point in the test life-cycle the test will be resumed.

If the NE provides the capability to schedule the test execution within a time window, then it shall be possible, from the OS, to set up the boundaries of the time window with a start time and a stop time. The start time is the earliest time at which the test performer can start the test execution (the actual starting time depends on the current conditions of the NE during the time window). The stop time is the latest time at which the test execution shall be ended; the actual stop time, however, depends on when the test was actually started and usually it should be reached before the stop time. The NE may also provide the capability to schedule the time to perform the initialization of the tests and the time window to perform the real test execution. In any case, the test performer has to provide complete information to the OS about the actual initialization time and execution time, together with the test results. In case the NE cannot perform the test within the time window, the OS shall be informed.

The NE may provide the test results in two ways: by means of test results reports or by means of TOs attributes; the latter way is possible only for controlled tests: in that case the test performer puts the results in some attributes of the TO and informs the test conductor that tests are completed; the operator at the OS can read the test results using basic common service which allows to get any attribute value from the NE. In any case, no matter how the test results are provided, they shall be very clear and shall contain all the information necessary to localize and to repair faults, if any. This information should include the objects that have been tested (MORTs), the Associated Objects (AOs), the Test Objects (TO), a clear test outcome which specifies if the test passed or failed or was terminated for some reason, a proposed repair action, etc. If, for any reason, a test is terminated, the partial results so far collected should be reported to the OS.

4.5.1.4.2 TMN Management Functions (ITU-T Recommendation X.745 [32])

1) **Request test** - Manager requests agent to perform a test: (B,E,F,G).
2) **Suspend/Resume test** - Manager instructs Agent to suspend/resume a test: (B,E,F,G).
3) **Terminate test** - Manager requests Agent to terminate a test: (B,E,F,G).
4) **Schedule test** - Manager provides Agent with a time window in which a test should be performed: (H).
5) **Request Test Results** – Manager requests Agent to report intermediate or final results from a measurement: (H).

6) **Test Results Reporting** – Agent sends the results of a test to the Manager: (H).

4.5.2 Configuration management

Configuration management provides functions to exercise control over, identify, collect data from and provide data to NEs, (ITU-T Recommendation M.3400 [8]).

4.5.2.1 Installation

Installation for the management of physical resources includes the following management function sets:

- NE installation administration function set (ITU-T Recommendation M.3400 [8]);
- installation completion reporting function set (ITU-T Recommendation M.3400 [8]).

4.5.2.1.1 NE installation administration

4.5.2.1.1.1 General Functional Model

NE installation administration provides access to information about the co-ordination of hardware and software for new installation, upgrades, and maintenance changes for individual NEs or a collection of NEs.
(ITU-T Recommendation M.3400 [8]).

Installation of equipment into a NE may require that management functions are available to support the operations. The actual process that the network operator adopts for installation (co-ordination between physical installation of equipment and OS related operations) is out of the scope of the present document. However, depending on how the installation process is organized, the OS may perform actions related to installation on the NE and the NE may notify the OS about the undergoing operations.

Managed object instances for the underlying installed physical resources shall be created either automatically by the NE or via an OS action during the installation process. It is part of this process the setting of all relevant attributes that define the location of the physical resource in the NE and the connectivity existing between the physical resource being installed and other resources in the NE. The installation process may also require the configuration of specific attributes related to the physical resource functionalities (subclause 4.5.2.2, "Provisioning" of the present document).

The physical resource being installed shall undergo testing operations before being made available for service. Tests may be performed either automatically by the NE or they may be requested by the OS. For OS requested tests and the reporting of automatically performed tests, the general functional model is the one defined in subclause 4.5.1.4, "Testing" of the present document.

The installation process may also require changes in the state and status attributes of the instanciated objects which model the underlying physical resources. The general functional model is the one defined in subclause 4.5.2.3, "Status and control" of the present document.

4.5.2.1.1.2 TMN Management Functions (ITU-T Recommendation X.730 [24])

1) **Create physical resource** - Manager directs Agent to create an instance of a physical resource: (A,B,C,D,E,F,G).

2) **Delete physical resource** - Manager directs Agent to delete an instance of a physical resource: (A,B,C,D,E,F,G).

3) **Notify physical resource creation** - Agent notifies manager that an instance of a physical resource has been created: (A,B,C,D,E,F,G).

4) **Notify physical resource deletion** - Agent notifies manager that an instance of a physical resource has been deleted: (A,B,C,D,E,F,G).

5) **Set physical resource attributes** - Manager requests Agent to set attributes on a physical resource: (A,B,C,D,E,F,G).

6) **Notify attribute value change** - Agent notifies Manager that attribute values on a physical resource have changed: (A,B,C,D,E,F,G).

4.5.2.1.2 Installation completion reporting

4.5.2.1.2.1 General Functional Model

Installation completion reporting provides access to information about job status and supports notification of completion after acceptance testing as required. It also supports notification of failure to meet successful completion criteria, with the reason for unsuccessful completion. It also supports summary and exception reports for the management of installation jobs, (ITU-T Recommendation M.3400 [8]).

4.5.2.1.2.2 TMN Management Functions

1) **Request installation completion report** - Manager requests Agent an installation completion report: (H).

2) **Request installation jobs summary** - Manager requests Agent the installation jobs summary: (H).

3) **Delete installation jobs summary** - Manager requests Agent to delete the installation jobs summary: (H).

4.5.2.2 Provisioning

Provisioning for the management of physical resources includes the following management function sets:

- NE(s) configuration function set (ITU-T Recommendation M.3400 [8])
- NE(s) inventory management function set
- Change over function set (ITU-T Recommendation X.751 [20])

4.5.2.2.1 NE(s) configuration

4.5.2.2.1.1 General Functional Model (GFM)

NE configuration supports the management and assignment of resources, available from an inventory, to a specific physical or administrative entity configuration. The supported functions allow to request the current configuration of an entity, its status, optional parameters, etc. The general functional model supports the installation, removal and monitoring of entities and the assignment and deletion of physical resources to entities. NE configurations supports also the modification specific of entity attributes.

The management of state and status attributes for physical resources is done according to subclause 4.5.2.3, "Status and control" of the present document.

The definition of relationships between resources for the purpose of configuration management makes use of the methods and models for relationships defined in ITU-T Recommendation X.732 [26] and/or ITU-T Recommendation X.725 [23].

4.5.2.2.1.2 TMN Management Functions (ITU-T Recommendation M.3400 [8])

1) **Request configuration** – Manager requests that the Agent report the current configuration of each entity: (A,B,C,D,E,F,G).

2) **Configuration report** – For each entity, Agent reports status, capacity of the entity, optional parameters, type of entity (in sufficient detail for Manager identification) and the version and revision of the version: (A,B,C,D,E,F,G)

3) **Grow** - Manager notifies Agent of the presence of a newly installed entity: (A,B,C,D,E,F,G).

4) **Prune** - Manager notifies Agent of the disconnection of an entity: (A,B,C,D,E,F,G).

5) **Restore** – Manager notifies Agent to begin monitoring the newly installed entity: (A,B,C,D,E,F,G).

6) **Assign** - Manager notifies Agent that a previously unequipped entity is now equipped: (A,B,C,D,E,F,G).

7) **Delete** - Manager notifies Agent that a previously equipped entity is no longer equipped: (A,B,C,D,E,F,G).

8) **Request assignments** – Manager requests that Agent report the identity of each assigned entity. The request may be for a specified entity or for all equipped entities: (A,B,C,D,E,F,G).

9) **Assignment reports** – Agent reports the identity of each assigned entity for each equipped entity or for a specified entity: (H).

10) **Set parameters** – Manager directs Agent to set parameters associated with a specified entity: (A,B,C,D,E,F,G).

11) **Set report periods** – The Manager directs Agent to set or change report periods: (H).

12) **Request report periods** – The Manager requests Agent to send the current periods to the Manager: (H).

NOTE: clauses from 3 to 7 need to be clarified.

4.5.2.2.2 NE(s) inventory management

4.5.2.2.2.1 General Functional Model

NE inventory management supports requests for availability status from resources, requests for the selection and assignment of those resources, requests for the resources to change service state, and reports the assignments, as appropriate. It also supports requests for counting and reporting the remaining idle resources and supports notifications that the value of counts of remaining idle resources has fallen below a pre-determined threshold,
(ITU-T Recommendation M.3400 [8])

NE(s) inventory notifications shall be emitted in relation to the sending of create, delete and attribute change events regarding either equipment or logical resources in a NE. The TMN management functions in this case are those defined in subclause 4.5.2.1 and in subclause 4.5.2.3, of the present document.

NE inventory management provides access to information about the current status of an NE and the features that the NE maintains. It also allows access to records of equipment or logical resources in order to perform queries to the inventory information.

The definition of relationships between resources for the purpose of configuration management makes use of the methods and models for relationships defined in ITU-T Recommendation X.732 [26]) and/or
(ITU-T Recommendation X.725 [23].

4.5.2.2.2.2 TMN Management Functions

1) **Find idle resource** - Manager requests Agent to find an idle physical resource: (A,B,C,D,E,F,G).

2) **Select idle resource -** Manager requests Agent to select an idle physical resource for assignment in a configuration: (A,B,C,D,E,F,G).

3) **Assign resource to configuration** - Manager requests Agent to assign a resource to a configuration: (A,B,C,D,E,F,G).

4) **Report resource assignment** - Manager requests Agent to report a resource assignment: (H).

5) **Request resource status** - Manager requests Agent the resource status: (H).

4.5.2.2.3 Change over (ITU-T Recommendation X.751 [20])

4.5.2.2.3.1 General Functional Model

The change over relationship is the composition of the fallback relationship and the back-up relationship and provides the back-up control function that makes a managed object that is fallbacked by one or more managed objects to be backed up by one of the fallbacking managed object based upon receiving the change over operation. The semantics of the fallback relationship and the back-up relationship is used to describe this relationship.

The semantics of fallback relationship is defined in subclause 7.3.3 of ITU-T Recommendation X.732 [26], as follows:

"A fallback relationship is an asymmetric relationship denoting that the second of a pair of managed objects (the secondary object) has been designated as a fallback or "next preferred choice" to the first managed object (the primary object). The existence of a fallback relationship implies that the secondary resource is capable of providing Back-up service to the primary resource if the latter is unable to fulfil its function. It does not necessarily imply that the secondary resource is currently active and performing its Back-up function in place of the primary resource.

Primary and secondary are two roles in a fallback relationship. A one-way fallback relationship exists if a managed object designates a second managed object to be in the secondary role, or if the second managed object designates the first managed object to be in the primary role. A reciprocal fallback relationship exists if both managed objects designate each other to be in the complementary roles.

The order of preference in which the secondary objects are selected to provide Back-up service to the primary object is expressed as a priority value attached to each secondary object.

The order of preference in which primary objects are selected for the provision of Back-up service by the secondary object is expressed as a priority value attached to each primary object."

The semantics of the back-up relationship is defined in 7.3.4 of ITU-T Recommendation X.732 [26], as follows:

"A back-up relationship is an asymmetric relationship denoting that the second of a pair of managed objects (the back-up object) is currently active and performing a back-up function in place of the first managed object (the backed-up object).

Back-up object and backed-up object are two roles in a back-up relationship. A one-way back-up relationship exists if a managed object designates a second managed object to be in the back-up role, or if the second managed object designates the first managed object to be in the backed-up role. A reciprocal back-up relationship exists if both managed objects designate each other to be in the complementary roles.

A back-up relationship is created as a result of a pre-existing fallback relationship between two managed objects. The back-up relationship comes into existence when the backed-up resource is not fulfilling its function, and the back-up resource is activated to provide the same service. The back-up resource ceases to provide that service. Creation and deletion of the back-up relationship has no effect on the existence of the fallback relationship between the two managed objects.

A backed-up object may be in the disabled or enabled operational state. The administrative state of the back-up object shall be unlocked to allow the back-up relationship to exist. When a managed object is being backed up for any reason (i.e. a back-up relationship exists), the back-up object is in use as long as it is not disabled. The operational and administrative states are defined in ITU-T Recommendation X.731 [25]."

The change over managed relationship class represents the managed change over relationship between managed object classes. This managed relationship class has the following roles:

- primary role;
- secondary role;
- backed-up role;
- back-up role;
- change over control role.

4.5.2.2.3.2 TMN Management Functions

1) **Establish change over relationship** - The change over relationship is established: (H) (ITU-T Recommendation X.751 [20]).

2) **Bind to secondary role** - At least one managed object is bound to the secondary role in the change over relationship: (H) (ITU-T Recommendation X.751 [20]).

3) **Unbind from secondary role** - Al least one managed object is unbound from the secondary role in the change over relationship: (H) (ITU-T Recommendation X.751 [20]).

4) **Terminate** - The change over relationship is terminated: (H) (ITU-T Recommendation X.751 [20]).

5) **Query** - Information regarding the change over relationship is requested: (H).
(ITU-T Recommendation X.751 [20]).

4.5.2.3 NE(s) status and control

4.5.2.3.1 General Functional Model

The TMN provides the capability to monitor and control certain aspects of the NE on demand. Examples include checking or changing the service state of a NE or one of its sub-parts (in service, out of service, standby). Normally, a status check is provided in conjunction with each control function in order to verify that the resulting action has taken place: (ITU-T Recommendation M.3400 [8]).

Status and control functions can also be part of routine maintenance when executed automatically or on a scheduled periodic basis: (ITU-T Recommendation M.3400 [8]).

NE(s) status and control provides access to the status of service resources and receives requests for transitions. Status information should be available to queries and should also be used to determine the legality of requested state changes: (ITU-T Recommendation M.3400 [8]).

This function set supports the reporting of changes of state as the result of recognition that a state has changed. Automatic notification of change of state may be initiated by the NE: (ITU-T Recommendation M.3400 [8]).

4.5.2.3.2 TMN Management Functions (ITU-T Recommendation M.3400 [8])

1) **Request status** – Manager requests Agent to send current status information: (A,B,C,D,E,F,G).

2) **Status report** – Agent reports to Manager the value of a monitored parameter. It may be sent on demand by Manager or on a scheduled basis: (H).

3) **Schedule status report** – Manager directs Agent to establish a schedule for the reporting of status information: (H).

4) **Request status report schedule** – Manager directs Agent to send the current schedule of status reporting agent responds with the schedule: (H).

5) **Allow/inhibit automatic restoration** – manager directs agent to allow or inhibit automatic restoration in an m:n or 1+1 system: (H).

6) **Control event report** – manager selects and controls the flow of notifications from the agent to the manager: (H).

5 Management information model

5.1 General introduction

5.1.1 Relationship with resources

The model maintains a relationship between the managed resources described in subclause 4.3 and the managed object classes defined in this chapter. Table 2 defines the correspondence between the two sets.

Table 2: Mapping between information model and physical resources.

Physical Resource	Information Model
Row, Rack, Subrack, Slot, Physical group	M.3100:equipmentHolder
Card, Storage device	M.3100:circuitPack
Power supply	ETS 300 304 Ed.2:powerSupply
Connector, Cable	modelled with conditional packages
Module	Module
Timing generator	ETS 300 304 Ed.2:timingGenerator
Timing receptor	ETS 300 304 Ed.2:timingPhysicalTerminationBidirectional
Sensor interface unit	externalInputPoint, externalOutputPoint

NOTE 1: Back panels with functionalities that request to be managed are not covered by the present document. The managed object class that would allow the modelling of this kind of equipment has been identified in ITU-T Recommendation M.3100 [13] : circuitPack. It should be noticed that the typical hierarchy of hardware resources requires that a back panel be contained either in a rack or in a subrack. From the modelling point of view this would require that an equipment holder (e.g. a rack or a subrack) contains both other equipment holders (e.g. subracks or slots) and a circuit pack (i.e. the back panel). However this is currently forbidden in the present version of ITU-T Recommendation M.3100 [13] by the following name binding behaviour definitions: equipmentHolder-equipmentHolderBeh, circuitPack-equipmentHolder-autoCreatedBeh and circuitPack-equipmentHolder-explicitlyCreatedBeh. Future versions of the present document will cover the subject according to the updates in ITU-T Recommendation M.3100 [13].

NOTE 2: The present document contains a specialization of the ITU-T Recommendation M.3100 [13]: equipmentHolder and ITU-T Recommendation M.3100 [13] : circuitPack object classes in order to allow the modelling of cables and connectors with conditional packages. The cables and connectors packages have been proposed to ITU-T Recommendation M.3100 [13] and will be included in future versions of the present document according to updates in the ITU-T Recommendation.

NOTE 3: Audio and visual indicators management according to ITU-T Recommendation Q.821 [14].

5.2 Entity Relationship

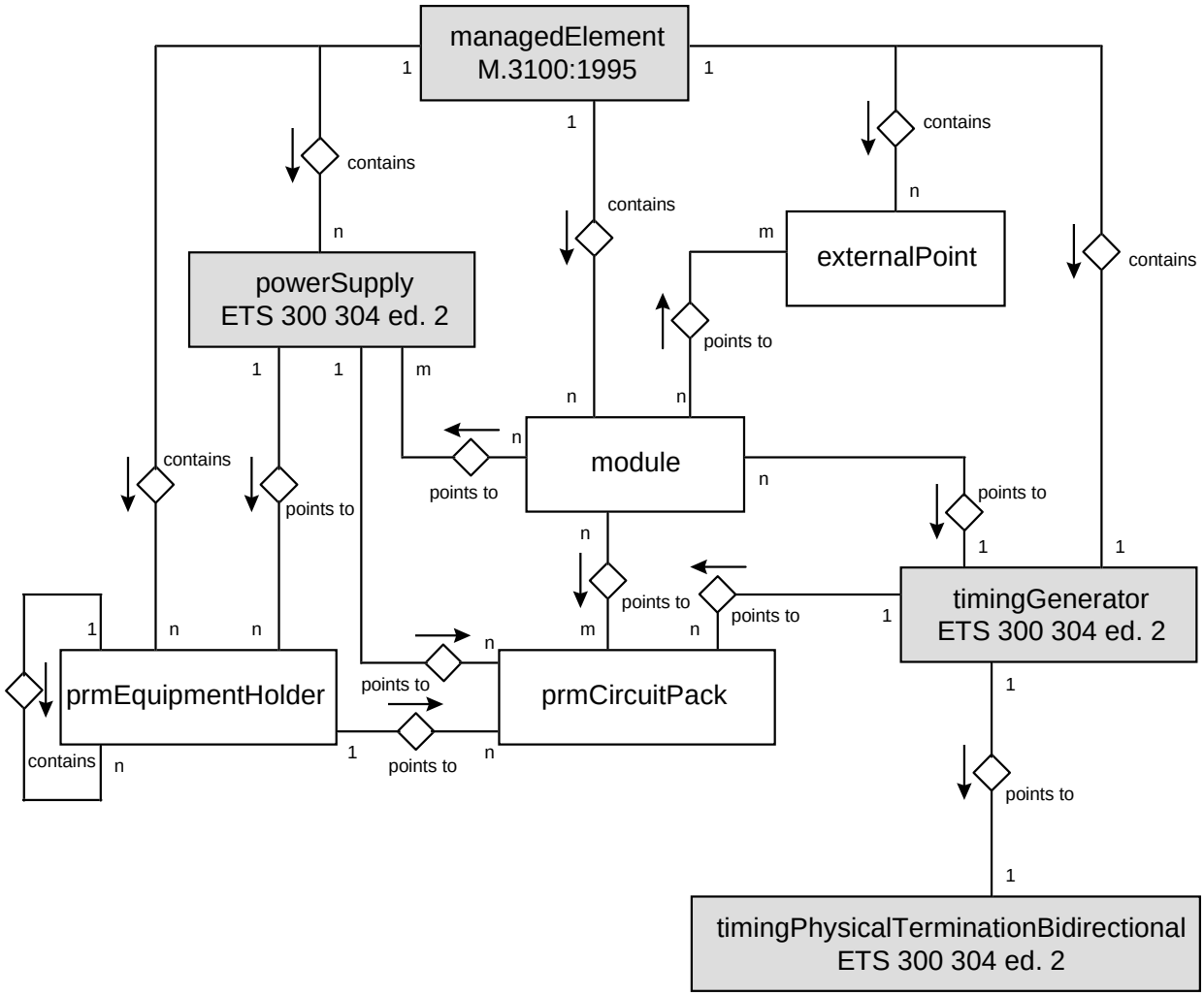

Figure 9: Entity relationship diagram.

NOTE: The shaded boxes in figures from 9 to 12 refer to managed object classes that are imported from other documents. The white boxes refer to object classes which are defined in the present document.

5.3 Inheritance Diagram

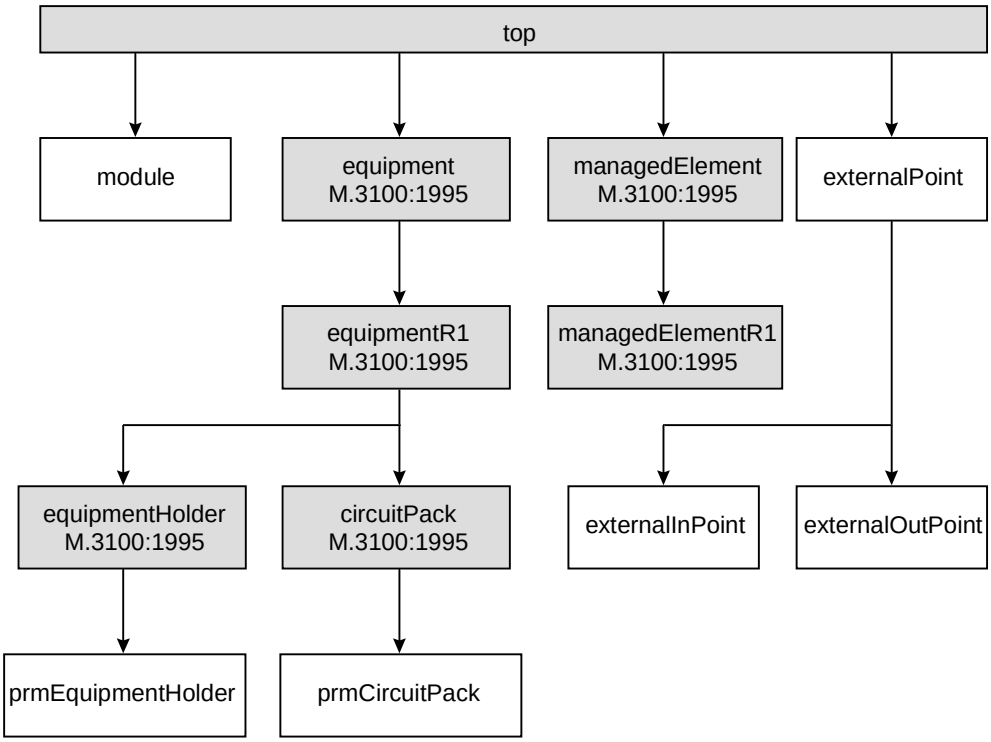

Figure 10: Inheritance diagram, part 1 of 2.

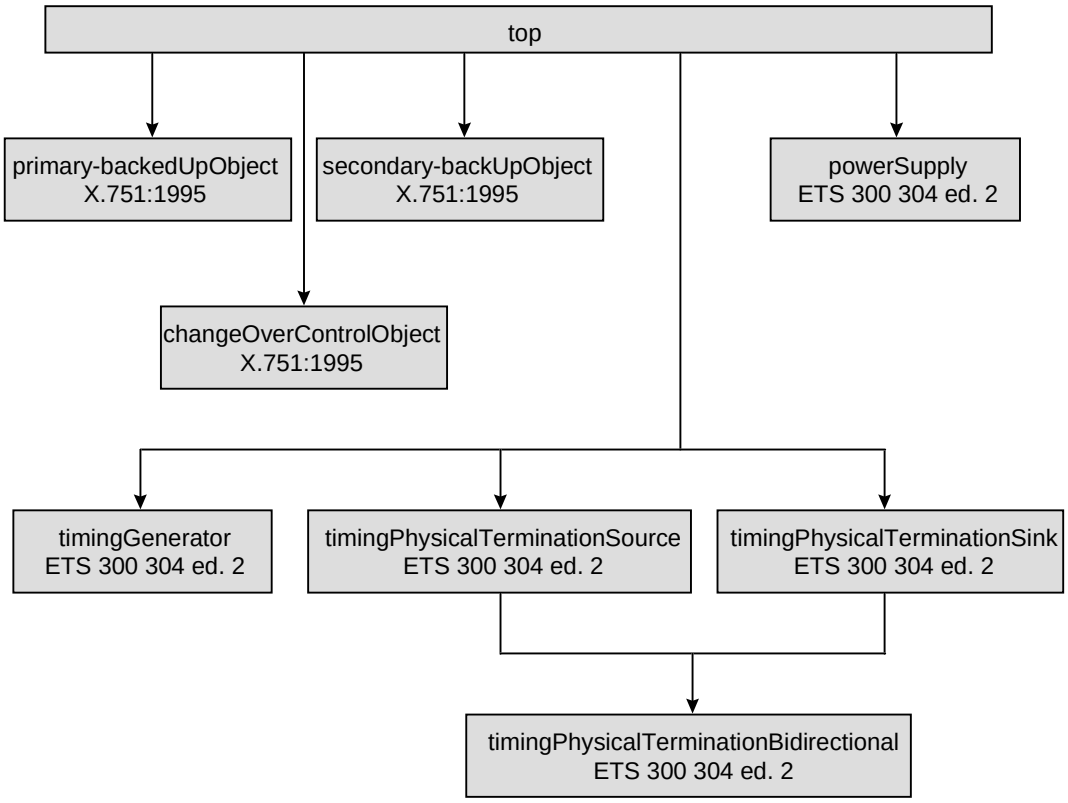

Figure 11: inheritance diagram part 2 of 2.

An alternative modelling of equipment sub-tree is in annex A.

An alternative modelling of redundancy/protection sub-tree is in annex B.

5.4 Containment Diagram

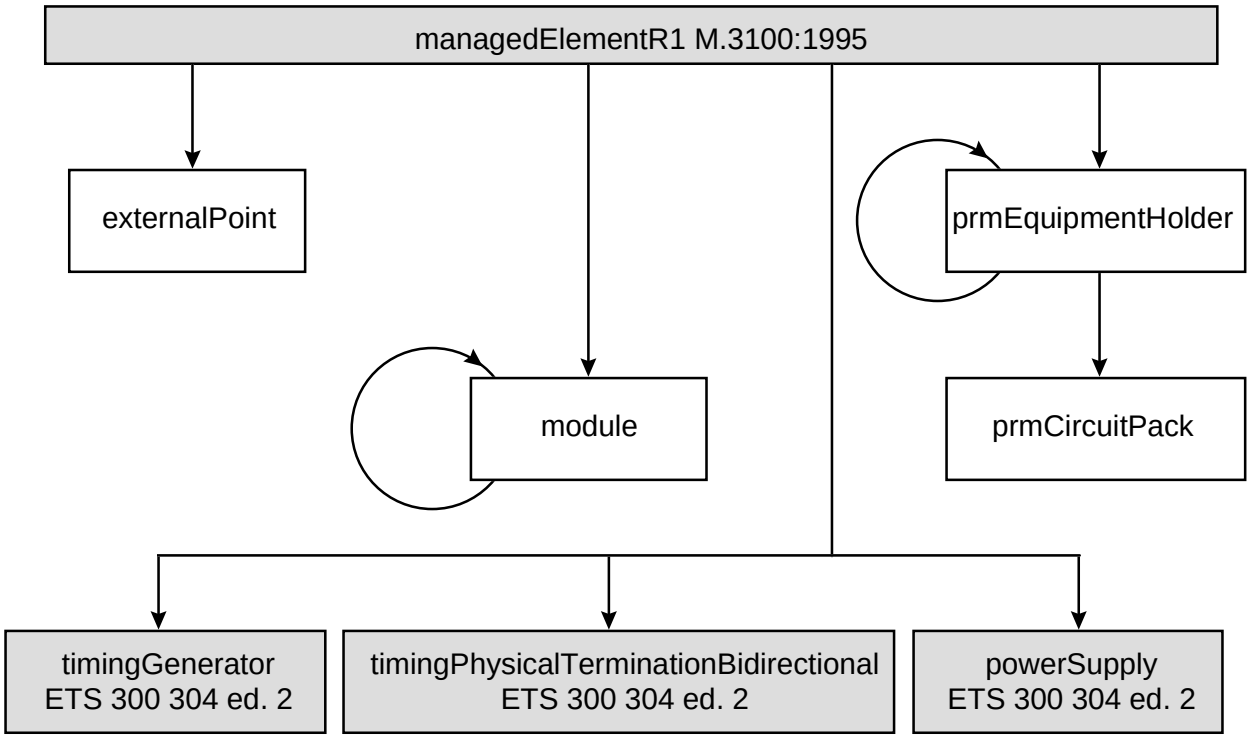

Figure 12: Containment diagram.

The above containment is appropriate for the NE to OS interface. For interfaces between OSFs other containment relationships may be appropriate.

5.5 Physical resources fragment

5.5.1 Managed object class definitions

The following managed object classes are imported from (ETS 300 304-2 [6]):

- powerSupply;
- timingPhysicalTerminationBidirectional;
- timingGenerator.

Additional managed object classes are defined in the following paragraphs.

5.5.1.1 PRM Circuit Pack

```
prmCircuitPack MANAGED OBJECT CLASS
    DERIVED FROM "M.3100:1995":circuitPack
    CONDITIONAL PACKAGES
        physicalConnectionPackage
            PRESENT IF "The resource identified by the circuit pack holds physical connectors and an
                    instance supports it.";
REGISTERED AS { managedObjectClass 1 }
```

5.5.1.2 PRM Equipment Holder

```
prmEquipmentHolder MANAGED OBJECT CLASS
    DERIVED FROM "M.3100:1995":equipmentHolder
    CONDITIONAL PACKAGES
        physicalConnectionPackage
            PRESENT IF "The resource identified by the equipment holder holds physical connectors
                       and an instance supports it.";
REGISTERED AS { managedObjectClass 2 }
```

5.5.1.3 Module

```
module MANAGED OBJECT CLASS
    DERIVED FROM "X.721:1992":top
    CHARACTERIZED BY
    modulePackage PACKAGE
        BEHAVIOUR
            moduleBehaviour BEHAVIOUR
            DEFINED AS
                "The Module object class is a class of managed objects putting in an administrative
                relation several physical entities. The related physical entities could be Hw
                entities, Sw entities or both together.
                The supportedByObjectList attribute contains the list of the related instances
                (i.e.: Circuit Pack, Software Unit, Module).
                The moduleType attribute allows to create a classification between the instances of
                the class according to a user-specified criteria (e.g.: the supported
                functionalities).
                The version attribute is related to the Module instance version that could be
                affected but it is not strictly related to the physical entities versions.
                The modules states are affected by the supported object state transition in the
                following way:
                If the LOCKED/DISABLE resource is unique and essential for the whole module
                its locking/disabling implies the changing of the OPERATIONAL status to DISABLE.
                If the LOCKED/DISABLED resource is duplicated (e.g.: Module Protected) this has no
                direct consequences on the states but only a general reduction of the module
                capacity (currently not defined in the object). On the other side the locking of the
                module should directly affect in the same way the resources administrative states."

        ATTRIBUTES
        moduleId                                GET;
        moduleType                              GET;
        "M.3100:1995":supportedByObjectList     GET;
    CONDITIONAL PACKAGES
        "M.3100:1995":createDeleteNotificationPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":attributeValueChangePackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":stateChangeNotificationPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":affectedObjectListPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":userLabelPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":versionPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":currentProblemListPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":protectedPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":administrativeOperationalStatesPackage
            PRESENT IF "An instance support it. ",
        "M.3100:1995":alarmSeverityAssignmentPointerPackage
            PRESENT IF "An instance support it. ";
REGISTERED AS { managedObjectClass 3 }
```

5.5.1.4 External Point

```
externalPoint MANAGED OBJECT CLASS
    DERIVED FROM top;
    CHARACTERIZED BY
        "M.3100:1995":locationNamePackage,
        "M.3100:1995":createDeleteNotificationsPackage,
        "M.3100:1995":operationalStatePackage,
        "M.3100:1995":stateChangeNotificationPackage,
        "M.3100:1995":userLabelPackage,
        externalPointPackage PACKAGE
            BEHAVIOUR
                externalPointBehaviour BEHAVIOUR
                DEFINED AS
```

```
                "The external point object class is used to monitor and control external
                input/output points within the managed element.
                The locationName package is used to identify the physical location of the external
                point on the equipment (for connection purposes)
                The user label package is used to associate a user-friendly label with the external
                point.
                The polarity attribute is used by subclasses to relate the external state of the
                external point to its internal state.
                Instances of subclasses of this object class are automatically created/deleted by
                the managed element when the object instance associated with equipment is
                created/deleted.";;
            ATTRIBUTES
                externalPointId                     GET,
                "M.3100:1995":supportedByObjectList GET,
                polarity                            GET-REPLACE;;;
    CONDITIONAL PACKAGES
        "M.3100:1995":alarmSeverityAssignmentPointerPackage
            PRESENT IF "an instance supports it";
REGISTERED AS { managedObjectClass 4 };
```

5.5.1.5 External Input Point

```
externalInputPoint MANAGED OBJECT CLASS
    DERIVED FROM externalPoint;
    CHARACTERIZED BY
        "M.3100:1995":environmentalAlarmR1Package,
        externalInputPointPackage PACKAGE
            BEHAVIOUR
                externalInputPointBehaviour BEHAVIOUR
                DEFINED AS
                "The externalInputPoint object is used to monitor an input point on a managed
                element. There will be one instance for each input point supported by the managed
                element
                The polarity attribute is used to relate the state of the physical input to the
                external state attribute. Two types of input are considered - contact closure and
                logic level inputs. The effect of the polarity attribute is as follows
```

	Polarity = activeHigh	Polarity = activeLow
High Logic Level or Contact Open	externalState = on	externalState = off
Low Logic Level or Contact Closed	externalState = off	externalState = on

```
                An input point will generate an environmental alarm if the externalState is on , as
                determined by the polarity. The probable cause of the alarm that will be sent in the
                environmental alarm can be set by the management system. When this object is created
                the default value for the probableCause attribute shall be "indeterminate"
                A change in the externalState to On will generate an alarm notification. If the
                alarmSeverityAssignmentProfilePointer is NULL or not present, then the perceived
                severity shall be indeterminate.";;
            ATTRIBUTES
                externalState                   GET,
                "X.721":probableCause           GET-REPLACE;;;
            NOTIFICATIONS
                "M.3100:1995":environmentalAlarm;;;
REGISTERED AS { managedObjectClass 5 };
```

5.5.1.6 External Output Point

```
externalOutputPoint MANAGED OBJECT CLASS
    DERIVED FROM externalPoint;
    CHARACTERIZED BY
        externalOutputPointPackage PACKAGE
            BEHAVIOUR
                externalOutputPointPackageBehaviour BEHAVIOUR
                DEFINED AS
                "The externalOutputPoint object is used to control an output point on a managed
                element. There will be one instance for each output point supported by the managed
                element.
                The polarity attribute is used to relate the state of the physical output to the
                external state attribute. Two types of output are considered - contact closure and
                logic level outputs. The effect of the polarity attribute is as follows
```

	Polarity = activeHigh	Polarity = activeLow
externalState = on	High Logic Level or Contact Open	Low Logic Level or Contact Closed
	Low Logic Level	High Logic Level

externalState = off	or Contact Closed	or Contact Open

```
                The current state of the output point can be found by reading externalState
                attribute and the state can be changed using this attribute.
                If a "short-circuit" (or other problem) can be detected and the
                equipmentsEquipmentAlarmPackage is present, then it is reported as an equipment
                alarm with a probable cause of externalIFDeviceProblem";;
            ATTRIBUTES
                externalState               GET-REPLACE;;;
    CONDITIONAL PACKAGES
        "M.3100:1995":equipmentsEquipmentAlarmR1Package
            PRESENT IF "an instance supports it and the output point can detect short circuits (or
            other abuses) on the ouput point ";
REGISTERED AS { managedObjectClass 6 };
```

5.5.2 Packages Definition

5.5.2.1 Physical Connection

```
physicalConnectionPackage PACKAGE
    ATTRIBUTES
        physicalConnectorList       GET SET-BY-CREATE,
        physicalConnectionList      GET-ADD-REMOVE;
REGISTERED AS { package 1 };
```

5.5.3 Attributes Definition

5.5.3.1 External Point Id

```
externalPointId ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.NameType;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       externalPointIdBehaviour;
REGISTERED AS { attribute 1 };

externalPointIdBehaviour BEHAVIOUR
    DEFINED AS
    "This attribute is used to name instances of the external point managed object class ";
```

5.5.3.2 External State

```
externalState ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.OnOff;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       externalStateBehaviour;
REGISTERED AS { attribute 2 };

externalStateBehaviour BEHAVIOUR
    DEFINED AS
    "This attribute is used to describe the state of an external point.";
```

5.5.3.3 Polarity

```
polarity ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.Polarity;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       polarityBehaviour;
REGISTERED AS { attribute 3 };

polarityBehaviour BEHAVIOUR
    DEFINED AS
     "the polarity attribute is used to assign the sensing polarity of an input or output point.";
```

5.5.3.4 Module Id

```
moduleId ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.NameType;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       moduleIdBehaviour;
REGISTERED AS { attribute 4 };

moduleIdBehaviour BEHAVIOUR
```

```
    DEFINED AS
    "This attribute is used to name instances of the module managed object class ";
```

5.5.3.5 Module Type

```
moduleType ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.ModuleType;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       moduleTypeBehaviour;
REGISTERED AS { attribute 5 };

moduleIdBehaviour BEHAVIOUR
    DEFINED AS
    "This attribute is used to classify the module managed object class according their types.";
```

5.5.3.6 Physical Connector List

```
physicalConnectorList ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.PhysicalConnectorList;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       physicalConnectorListBehaviour;
REGISTERED AS { attribute 6 };

physicalConnectorListBehaviour BEHAVIOUR
    DEFINED AS
    "This attribute indicates the set of physical connectors supported by a physical resource.";
```

5.5.3.7 Physical Connection List

```
physicalConnectionList ATTRIBUTE
    WITH ATTRIBUTE SYNTAX       PhysicalResourceManagementModule.PhysicalConnectionList;
    MATCHES FOR     EQUALITY;
    BEHAVIOUR       physicalConnectionListBehaviour;
REGISTERED AS { attribute 7 };

physicalConnectionListBehaviour BEHAVIOUR
    DEFINED AS
    "This attribute is used to relate external cabling to the appropriate connectors (local and
         far). There is an entry per each local connector";
```

5.5.4 Name binding definitions

5.5.4.1 External Point - Managed Element

```
externalPoint-managedElement NAME BINDING
    SUBORDINATE OBJECT CLASS externalPoint AND SUBCLASSES;
    NAMED BY
    SUPERIOR OBJECT CLASS managedElement AND SUBCLASSES;
    WITH ATTRIBUTE      externalPointId;
REGISTERED AS { nameBinding 1 };
```

5.5.4.2 Module - Managed Element

```
module-managedElement NAME BINDING
    SUBORDINATE OBJECT CLASS module AND SUBCLASSES;
    NAMED BY
    SUPERIOR OBJECT CLASS managedElement AND SUBCLASSES;
    WITH ATTRIBUTE      moduleId;
REGISTERED AS { nameBinding 2 };
```

5.5.4.3 Module - Module

```
module-module NAME BINDING
    SUBORDINATE OBJECT CLASS module AND SUBCLASSES;
    NAMED BY
    SUPERIOR OBJECT CLASS module AND SUBCLASSES;
    WITH ATTRIBUTE      moduleId;
REGISTERED AS { nameBinding 3 };
```

5.5.5 ASN.1 Definitions

Rules of extensibility (ITU-T Recommendation M.3100 (13]) - The following types will be indicated as being extensible:

- ENUMERATED;
- named INTEGER;
- named BIT STRING;
- tagged SET;
- tagged SEQUENCE;
- tagged CHOICE;

Under the rules of extensibility new enumerations (for ENUMERATED types), new bit name assignments (for named BIT STRING types), new named numbers (for named INTEGER types), and new tagged elements (for tagged SET, SEQUENCE, and CHOICE types) may be added in future versions of this Recommendation. When processing information in a System Management Protocol (SMAP) PDU, the accepting SMAP machine shall ignore:

- enumerations not recognized;
- unrecognized named numbers;
- unrecognized named bits;
- unrecognized tagged elements of sets, sequences, and choices.

The ASN.1 productions defined in PhysicalResourceManagementModule conform to both the ASN.1 88-90 ITU-T Recommendation X.208 [15] version and the ASN.1 1994 ITU-T Recommendation X.680 [16-19] version.

```
PhysicalResourceManagementModule {ccitt(0) identified-organization(4) etsi(0) ets(x)
            informationModel(0) asn1Module(2) physicalResourceManagementModule(???)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- EXPORTS everything

IMPORTS

NameType FROM ASN1DefinedTypesModule {ccitt(0) recommendation(0) m(13) m3100(3100)
            informationModel(0) asn1Module(2) asn1DefinedTypesModule(0)};

-- OBJECT IDENTIFIER DEFINITIONS

informationModel    OBJECT IDENTIFIER ::= {ccitt(0) identified-organization(4) etsi(0) ets(x)
            informationModel(0) }
managedObjectClass      OBJECT IDENTIFIER ::= { informationModel managedObjectClass(3) }
package                 OBJECT IDENTIFIER ::= { informationModel package(4) }
parameter               OBJECT IDENTIFIER ::= { informationModel parameter(5) }
nameBinding             OBJECT IDENTIFIER ::= { informationModel nameBinding(6) }
attribute               OBJECT IDENTIFIER ::= { informationModel attribute(7) }
attributeGroup          OBJECT IDENTIFIER ::= { informationModel attributeGroup(3) }
action                  OBJECT IDENTIFIER ::= { informationModel action(9) }
notification            OBJECT IDENTIFIER ::= { informationModel notification(10) }

-- TYPE DEFINITIONS

Connected ::= SEQUENCE {
                cableType               [0] PrintableString,
                farEndConnectorList     [1] FarEndConnectorList
        }

Connection ::= CHOICE {
                notConnected    NULL,
                connected       Connected
        }
```

```
Connector ::= SEQUENCE {
                connectorType           [0] PrintableString,
                connectorIdentifier     [1] NameType
        }

FarEndConnectorList ::= SEQUENCE {
                farEndResource      [0] OBJECT IDENTIFIER,
                connectorList       [1] PhysicalConnectorList
        }

ModuleType ::= CHOICE {
                globalValue OBJECT IDENTIFIER,
                localValue  INTEGER
        }

OnOff ::= ENUMERATED {
                off (0),
                on  (1)
        }

PhysicalConnectionList ::= SEQUENCE OF Connection

PhysicalConnectorList ::= SEQUENCE OF Connector

Polarity ::= ENUMERATED {
                activeLow       (0),
                activeHigh      (1)
        }

END
```

5.6 Support fragment

The following managed relationship is imported from ITU-T Recommendation X.751 [20]:

- changeOverRelationship

The following managed object class is imported from ITU-T Recommendation M.3100 [13]:

- alarmSeverityAssignmentProfile

The following managed object classes are imported from ITU-T Recommendation Q.821 [14]:

- currentAlarmSummaryControl
- managementOperationsSchedule

The following managed object classes are imported from ITU-T Recommendation X.721 [21]:

- alarmRecord
- attributeValueChangeRecord
- eventForwardingDiscriminator
- log
- objectCreationRecord
- objectDeletionRecord
- relationshipChangeRecord
- securityAlarmReportRecord
- stateChangeRecord

The following managed object classes are imported from ITU-T Recommendation X.737 [30]:

- connectionTestObject

- connectivityTestObject
- dataIntegrityTestObject
- loopbackTestObject
- protocolIntegrityTestObject
- resourceBoundaryTestObject
- resourceSelfTestObject
- testInfrastructureTestObject

The following managed object classes are imported from ITU-T Recommendation X.738 [31]:

- bufferedScanner
- bufferedScanReportRecord
- dynamicSimpleScanner
- heterogenousScanner
- simpleScanner
- scanReportRecord

The following managed object classes are imported from ITU-T Recommendation X.745 [32]:

- schedulingConflictRecord
- testActionPerformer
- testObject
- testResultsRecord

The following managed object classes are imported from ITU-T Recommendation X.746 [22]:

- dailyScheduler
- weeklyScheduler
- monthlyScheduler
- periodicScheduler
- dailyOperationScheduler
- weeklyOperationScheduler
- monthlyOperationScheduler
- periodicOperationScheduler
- operationResultRecord

The following managed object classes are imported from ITU-T Recommendation X.751 [20]:

- primary-backedUpObject
- secondary-backUpObject
- changeOverControlObject

6 Protocol implementation

6.1 Service definitions

The present document makes use of the services defined in other management functions and does not define any additional services.

6.2 Functional units

6.2.1 Functional units defined in the present document

The following functional units are defined in the present document for the management of physical resources:

a) installation administration functional unit;

b) installation completion reporting functional unit;

c) configuration functional unit;

d) inventory management functional unit;

e) status and control functional unit.

Each functional unit requires the support of a number of services for instances of managed object classes. Table 3 summarizes functional units definitions.

Table 3: Functional units defined in the present document.

Management Area	Functional unit	Service	Managed Object Classes
Physical resources management	Installation administration	PT-SET PT-GET PT-ACTION PT-EVENT-REPORT Object creation/deletion reporting Attribute value change reporting	Module Equipment holder Circuit pack External input/output point Power Supply Timing generator Timing physical termination bi-directional Object creation record Object deletion record Attribute value change record
	Installation completion reporting	Activate scan report Scan report	Simple scanner Scan Report Record
		Activate dynamic simple scan report Scan report	Dynamic simple scanner Scan Report Record

Table 3 (continued)

Management Area	Functional Unit	Service	Managed Object Classes
Physical resources management (continued)	Configuration	Object creation/deletion reporting Attribute value change reporting State change reporting Relationship change reporting	Module Equipment holder Circuit pack External input/output point Power Supply Timing generator Timing physical termination bi-directional Protection group Protection unit Object creation record Object deletion record Attribute value change record State change record Relationship change record Scheduler
		Activate scan report Scan report	Simple scanner Scan Report Record
		Activate dynamic simple scan report Scan report	Dynamic simple scanner Scan Report Record
	Inventory management	State change reporting Relationship change reporting	Module Equipment holder Circuit pack External input/output point Power Supply Timing generator Timing physical termination bi-directional State change record Relationship change record

Table 3 (concluded)

Management Area	Functional Unit	Service	Managed Object Classes
Physical resources management (continued)	Status and control	State change reporting	Module Equipment holder Circuit pack External input/output point Power Supply Timing generator Timing physical termination bi-directional Protection group Protection unit State change record Scheduler

6.2.2 Functional units from other standards

The functional units indicated in table 4 may be negotiated for the purpose of managing physical resources.

Table 4: Functional units from other standards.

Management Area	Functional Unit	Service	Managed Object Classes
ITU-T Recommendation X.730 [24] Object management	allEvents	All notifications See note 1 below	
	control	All services except notificationsSee note 2 below	
	monitor	PT-GET only	
	objectEvents	Object creation reporting Object deletion reporting Attribute value change reporting	Object creation record Object deletion record Attribute value change record
ITU-T Recommendation X.731 [25] State management	State change reporting	State change reporting	State change record
ITU-T Recommendation X.732 [26] Attributes for representing relationship	Relationship change reporting	Relationship change reporting	Relationship change record
ITU-T Recommendation X.733 [27] Alarm reporting	Alarm reporting	Alarm reporting	Alarm record
ITU-T Recommendation X.734 [28] Event report	Event report management	PT-GET PT-SET PT-CREATE PT-DELETE Object creation/deletion reporting Attribute value change reporting State change reporting	Event forwarding discriminator
	Monitor event report management	PT-GET	Event forwarding discriminator

NOTE 1: All systems management notification services which map onto the CMIS M-EVENT-REPORT service. This includes the PT-EVENT-REPORT service defined in ITU-T Recommendation X.730 [24] as well as systems management notifications services defined by other systems management standards.

NOTE 2: All systems management notification services which map onto the CMIS M-GET, M-SET, M-ACTION, M-CREATE and M-DELETE services. This includes the PT-GET, PT-SET, PT-ACTION, PT-CREATE and PT-DELETE services defined in ITU-T Recommendation X.730 [24] as well as systems management services (except notifications services) defined by other systems management standards.

Table 4 (continued)

Management Area	Functional Unit	Service	Managed Object Classes
ITU-T Recommendation X.735 [29] Log control function	Log control	PT-GET PT-DELETE	Log Log record
		PT-SET PT-CREATE Object creation/deletion reporting Attribute value change reporting State change reporting Alarm reporting	Log
	Monitor log	PT-GET	Log Log record
ITU-T Recommendation X.738 [31] Summarization function	Scan stimulation	Activate scan report	Simple scanner Scan Report Record
		Report buffer	Buffered scanner Buffered scan report record
		Activate dynamic simple scan report	Dynamic simple scanner Scan Report Record
	Summarization event reporting	Scan report	Dynamic simple scanner Simple scanner Scan Report Record
		Buffered scan report	Buffered scanner Buffered scan report record
ITU-T Recommendation X.745 [32] Test management	Uncontrolled test	Test request uncontrolled	Test action performer
	Controlled test	PT-GET PT-SET PT-DELETE Test result	Test object Test results record
		Test request controlled Test suspend/resume Test terminate	Test action performer
		Scheduling conflict	Scheduling conflict record

Table 4 (concluded)

Management Area	Functional Unit	Service	Managed Object Classes
ITU-T Recommendation X.751 [20] Change over	Change over	Change over request	Change over control object
	Change over/back	Change over request Change back request	Change over control object
ITU-T Recommendation Q.821 [14] Alarm surveillance	Kernel	Alarm reporting	Event forwarding discriminator
	Basic alarm report control	Suspend/resume alarm reporting	Event forwarding discriminator
	Enhanced alarm report control	Initiate/terminate alarm reporting Set/get event forwarding discriminator	Event forwarding discriminator
	Alarm report retrieval	Alarm report retrieving	Log alarm record
	Alarm report deletion	Alarm report deleting	Log alarm record
	Current alarm summary reporting	Current alarm summary reporting	Management operations schedule Current alarm summary control
	Basic management operations scheduling	Suspend/resume management operations schedule	Management operations schedule
	Enhanced management operations scheduling	Initiate/terminate/set/get management operations schedule	Management operations schedule
	Current alarm summary reporting control	Initiate/terminate/set/get current alarm summary control	Current alarm summary control
	Current alarm summary retrieval	Retrieve current alarm summary	Current alarm summary control
	Alarm event criteria management	Initiate/terminate/set/get alarm severity assignment profile	Alarm severity assignment profile
	Alarm indication management	Inhibit/allow audible and visual local alarms Reset audible alarm	Managed element or its subclasses
	Basic log control	Suspend/resume logging	Log alarm record
	Enhanced log control	Initiate/terminate log Get/set log	Log alarm record

7 Scenarios

This clause contains some example scenarios for physical resource management, taken from ITU-T Recommendation M.3400 [8]. In all figures the shaded area represents the management functions dealt with by physical resource management.

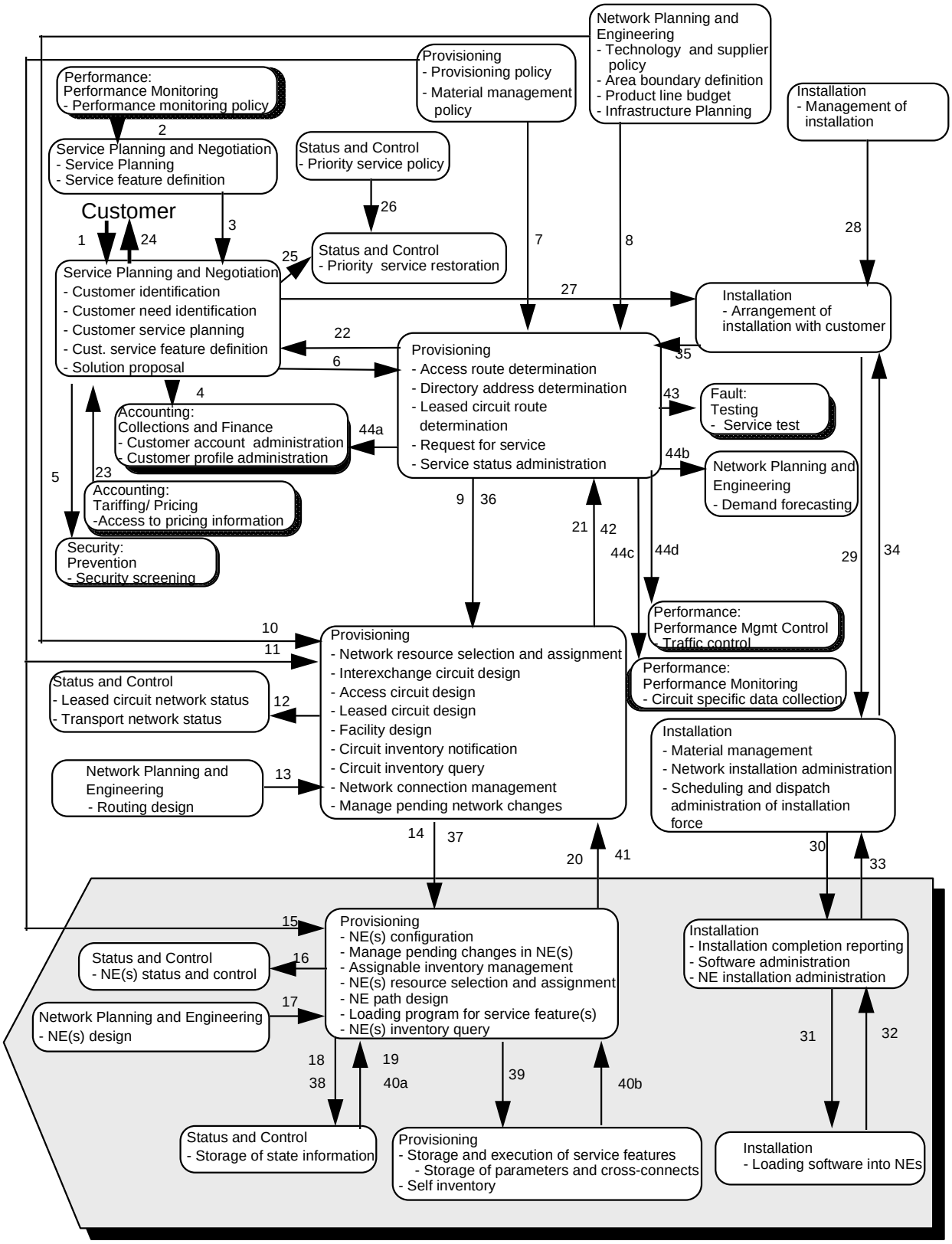

Figure 13: Service activation (figure I-1/M.3400).

Figure 13 is a possible scenario of service activation. Physical resource configuration management is involved with all management functions, including installation of resources, provisioning of these resources and status and control management.

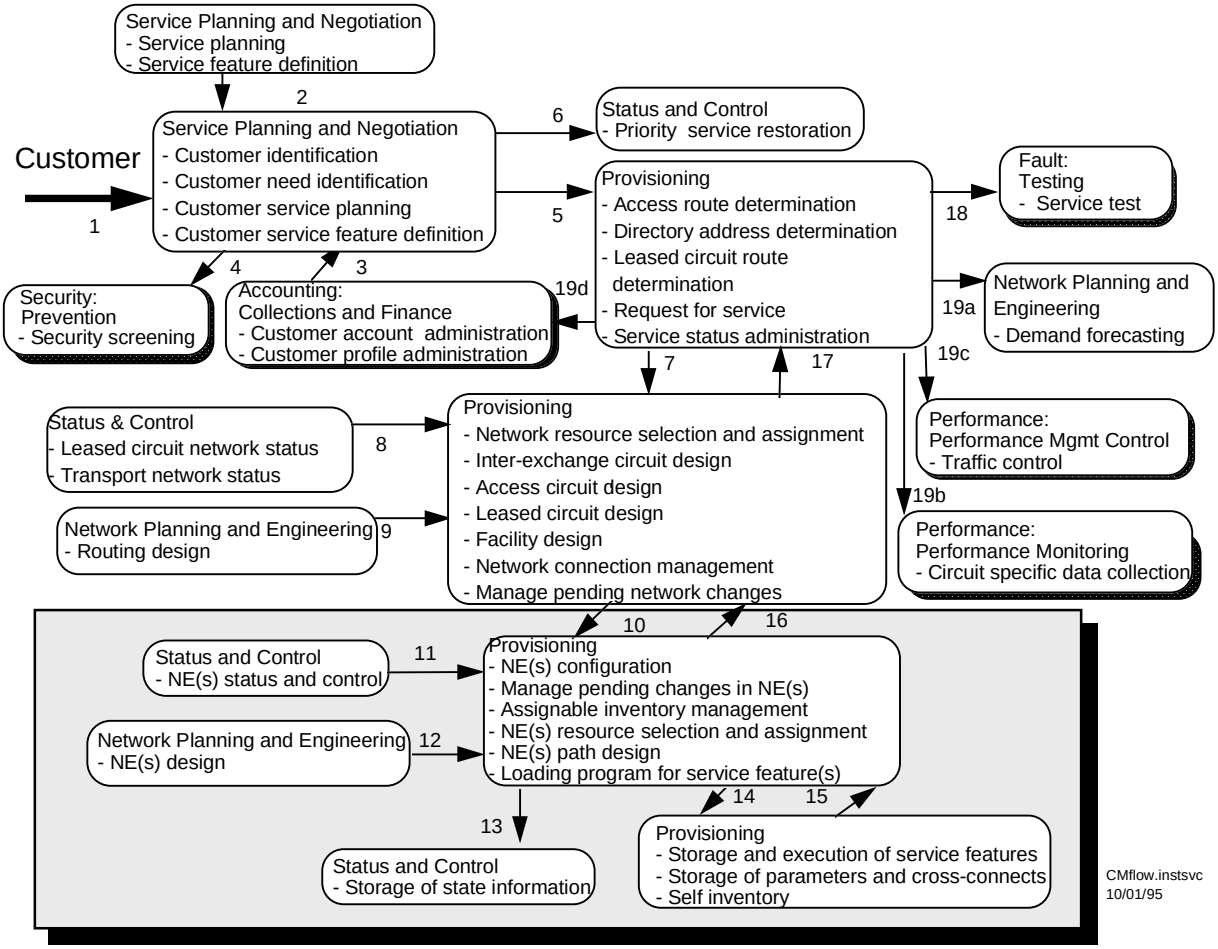

Figure 14: Immediate service activation with pre-equipped resources (figure I-2/M.3400).

Figure 14 is a somewhat simplified scenario in which service activation is requested with pre-equipped resources. In this case physical resource management makes use of provisioning and status and control management functions.

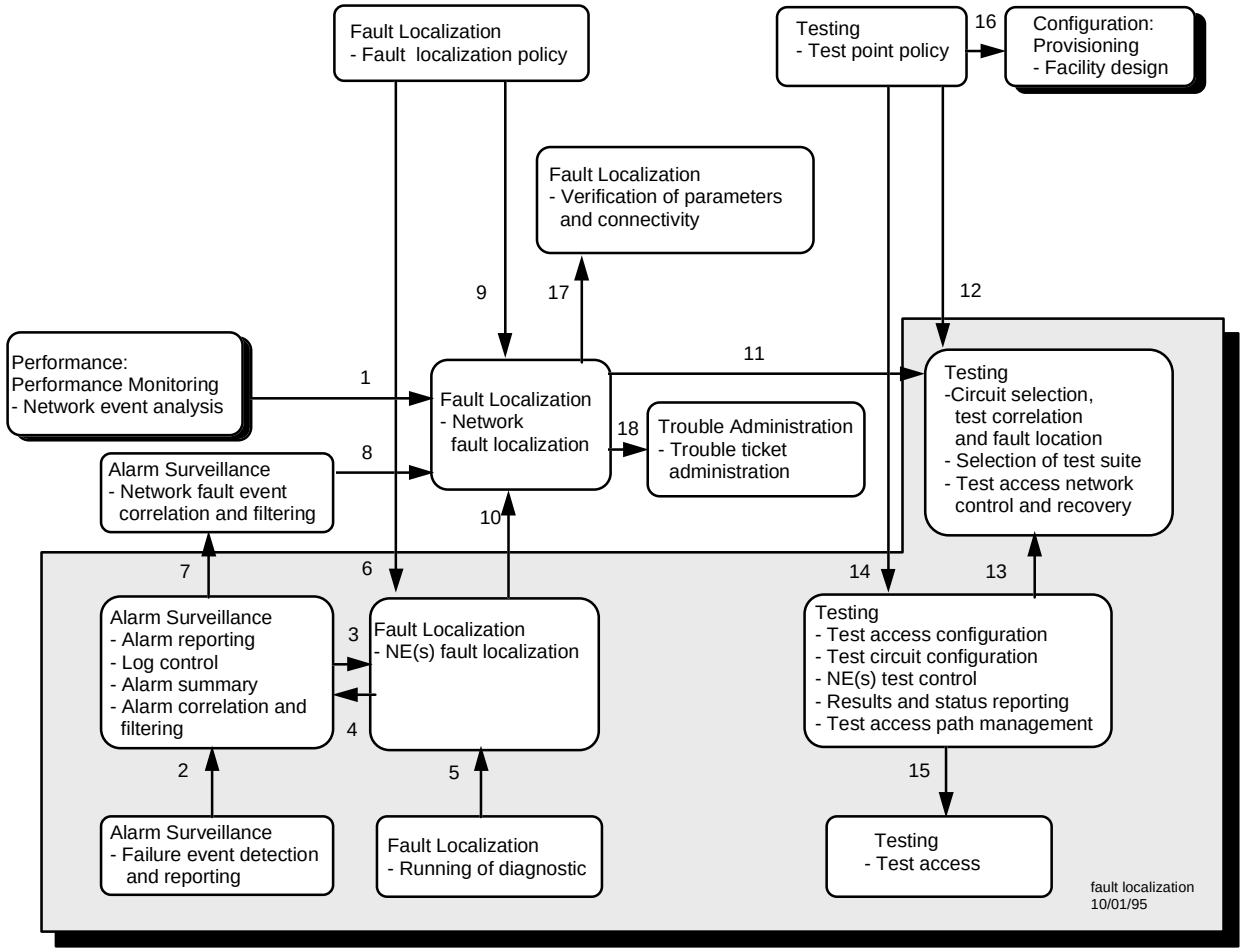

Figure 15: Fault localization (figure I-18/M.3400).

The scenario outlined in figure 15 includes management functions used in physical resource management and relating to alarm surveillance, fault localization and testing.

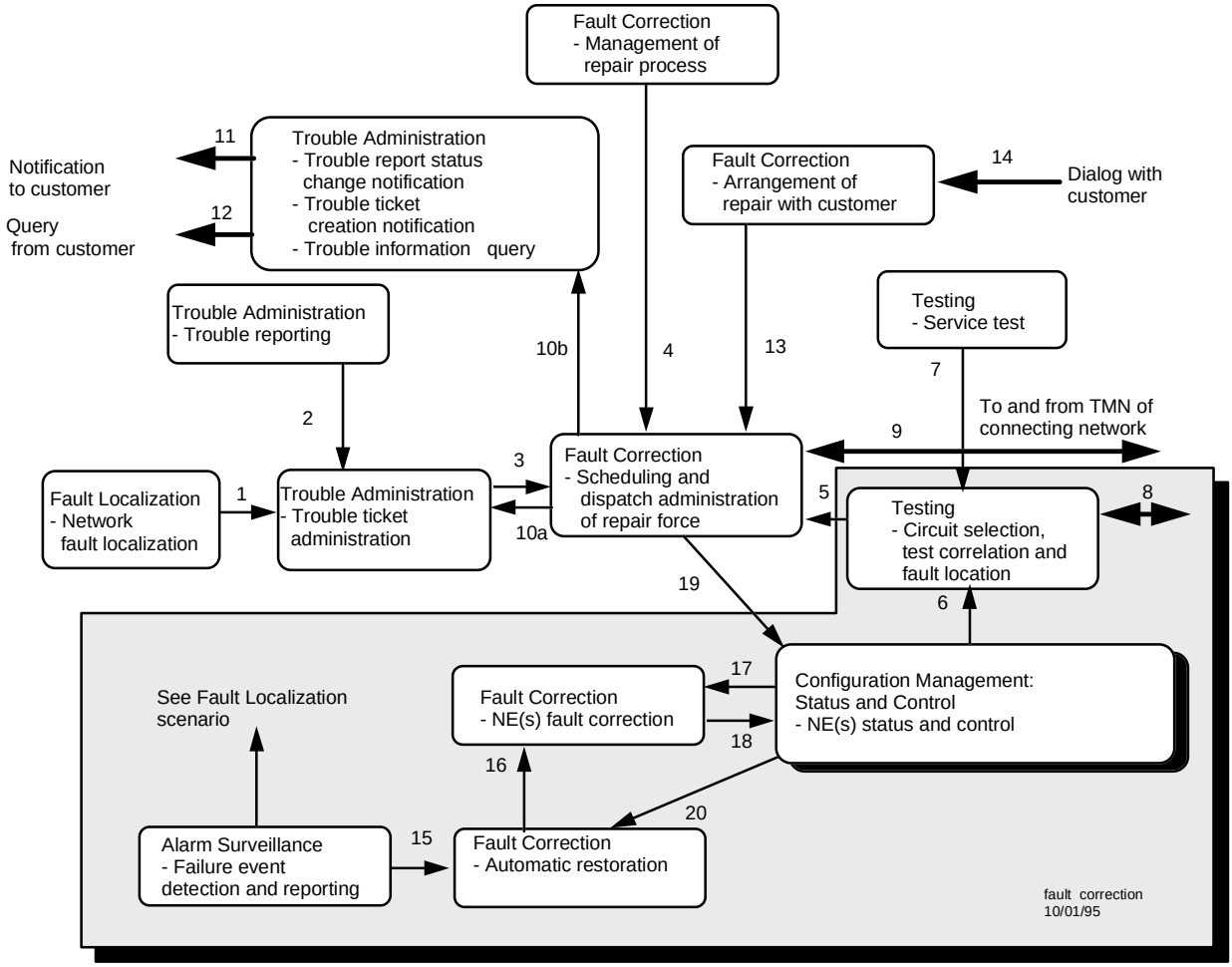

Figure 16: Fault correction (figure I-19/M.3400).

Figure 16 shows a fault correction scenario. Physical resource management requires functionalities not only in the fault correction area but also in the testing and configuration areas.

Annex A (normative): Alternative equipment sub-tree

A.1 Background

The equipment management sub-tree defined in ITU-T Recommendation M.3100 [13] (*equipment, equipmentR1, equipmentHolder, circuitPack*) is adopted by the present document (see subclause 5.5.1, "Managed object class definitions").

Long before the appearance of ITU-T Recommendation M.3100 [13], ETSI STC TM2 (Transmission Network Management) developed an equipment management information model. This was first published in 1992 as part of the ETS 300 304 Ed.1 (SDH Information Model for the Network Element view).

The ETS 300 304 "equipment fragment" is as well based on M.3100 by defining a sub-class of the *equipment* managed object class (*sdhEquipment*). See inheritance and containment diagrams in Sec. A.2.1 and A.2.2.

ETSI STC TM2 reiterated the ETS 300 304 in 1995 (Ed. 2) [6] when only a minor addition was introduced in the revised *sdhEquipmentR* object class. The "equipment fragment" defined in the ETS 300 304 can therefore be considered as a mature and stable specification that has been used so far for standard TMN applications in SDH networks.

The ETS 300 304 "equipment fragment" is equivalent in terms of management functionalities to the M.3100 model and although the reference to the SDH technology in the class label of the *sdhEquipmentR* object the model is generic by nature and can be applied to different technological areas.

A.2 Alternative standard option for Management Information

The *sdhEquipmentR* object class defined in the ETS 300 304 has to be considered an alternative standard option that can be used instead of the M.3100 *equipmentR1, equipmentHolder* and *circuitPack* object classes.

The *sdhEquipmentR* model is inspired to the M.3100 concept of recursive containment between instances of the same class to model the physical structure of a network element (see containment diagram below).

The *sdhEquipmentR* can therefore be used to model the various physical levels of a network element (i.e. racks, sub-racks, cards, etc.). Specific types of equipment are expressed by attributes in a similar manner as specified in the M.3100 *equipmentHolder* and *circuitPack* objects.

A.2.1 Inheritance diagram

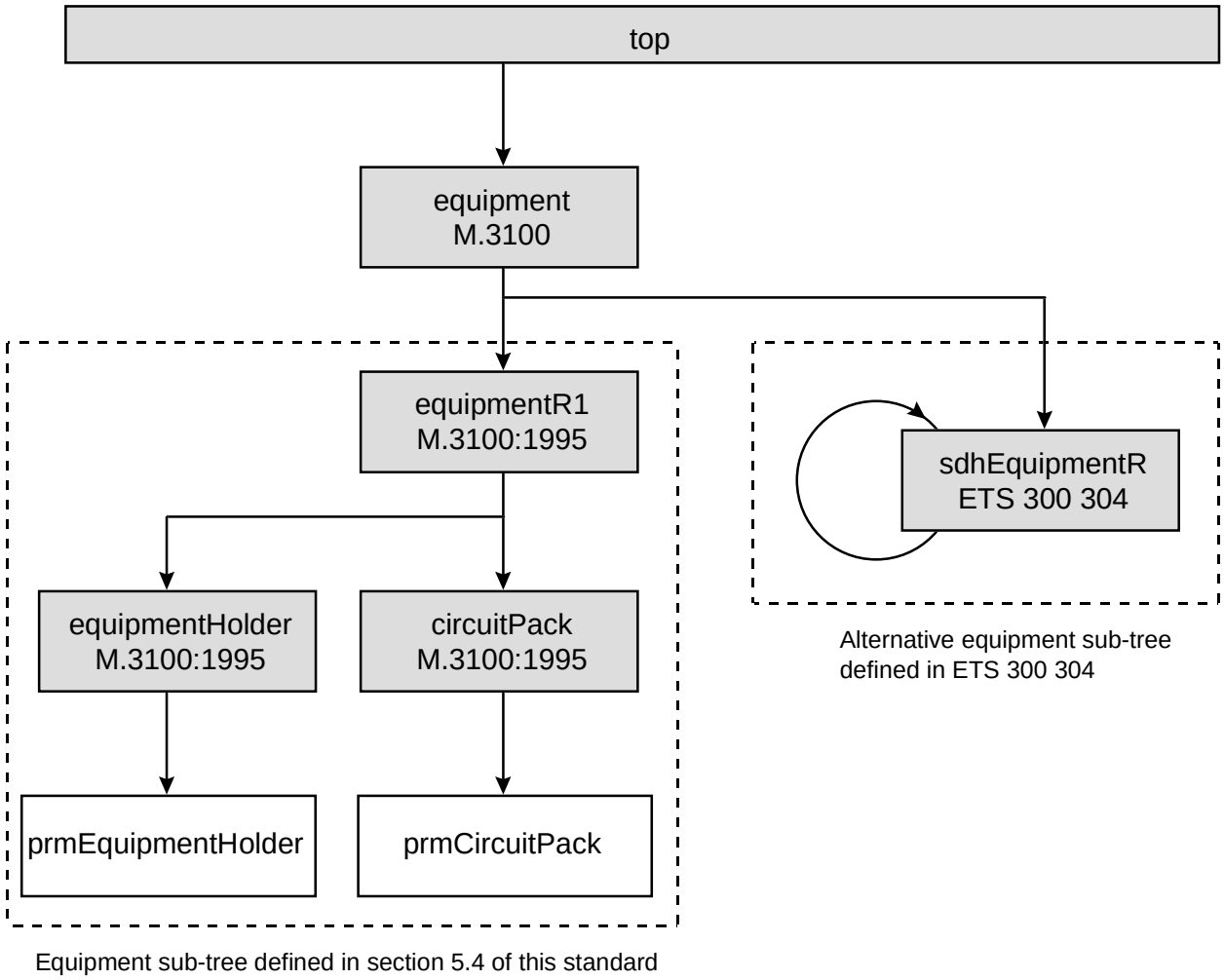

Figure 17: Alternative inheritance diagrams

A.2.2 Containment diagram

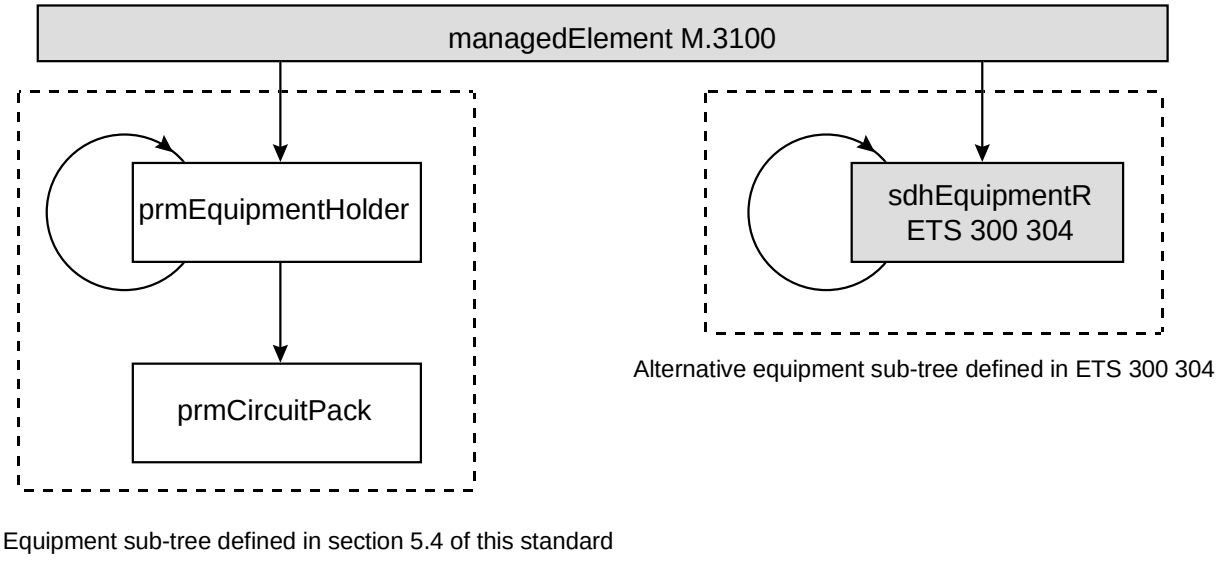

Figure 18: Alternative containment diagrams

NOTE: The shaded boxes in figures 17 and 18 refer to managed object classes that are imported from other documents. The white boxes refer to object classes which are defined in the present document.

A.2.3 Formal Object Class Definitions

A.2.3.1 Managed Object Classes

A.2.3.1.1 SdhEquipmentR

Imported from ETS 300 304 Ed.2 [6]

Annex B (normative): Alternative protection management sub-tree

B.1 Background

The change over management sub-tree defined in ITU-T Recommendation X.751 [20] is adopted by the present document. However this is not the only generic model for the management of equipment protection. The SDH series of standard have defined a generic information model for the management of protection operations. This annex contains the alternative model as an equally valid solution to the management protected physical resources.

B.2 Definitions

For the purpose of this annex the following definitions apply:

1:1: a fallback relationship with two resources involved. The secondary resource may perform additional work or be in a cold standby state (this definition is compatible with 1:1 protection architectures in SDH as defined in ITU-T Recommendation G.803 [10]).

1:n: a set of n fallback relationships where one secondary resource may act as back-up object for n primary objects. The secondary resource may perform additional work or be in a cold standby state. The order of preference in which the primary resources are selected for the provision of back-up service by the secondary resource is expressed by a priority value attached to each primary object. (ITU-T Recommendation X.732 [26]) (this definition is compatible with 1:n protection architectures in SDH as defined in ITU-T Recommendation G.803 [10])

1+1: a fallback relationship with two resources involved and where the secondary resource is in a hot standby state (this definition is compatible with 1+1 protection architectures in SDH as defined in ITU-T Recommendation G.803 [10]).

m:n: a set of fallback relationships where m secondary resources may act as back-up objects for n primary resources. The secondary resources may perform additional work or be in a cold standby state. The order of preference in which the secondary resources are selected to provide back-up service to the primary resource is expressed by a priority value attached to each secondary object. The order of preference in which the primary resources are selected for the provision of back-up service by the secondary resource is expressed by a priority value attached to each primary object. (ITU-T Recommendation X.732 [26]) (this definition is compatible with m:n protection architectures in SDH as defined in ITU-T Recommendation G.803 [10])

protection group: a protection group is a set of physical or administrative resources which define a protection relationship where one or more standby (i.e. backup) resources provide protection for one or more working (i.e. regular or preferred) resources.

protection unit: a protection unit represents a protected (i.e. working, regular or preferred) resource or a protecting (i.e.†backup or standby) resource.

B.3 TMN management context

B.3.1 Requirements

B.3.1.1 Fault management

B.3.1.1.1 Fault correction

Refer to subclause 4.4.1.3 of the present document.

B.3.1.2 Configuration management

B.3.1.2.1 Provisioning

For the purpose of equipment protection it shall be possible to (ITU-T Recommendation G.774-03 [9]):

- Manage a group of protected resources together with their protecting resources as one protection group, where all members of the protection group in a network element may be configured for:

  a) m:n or 1+1 type protection;

  b) revertive or non-revertive type switching;

  c) a specific wait-to-restore time (in the case of revertive systems).

- Indicate the ability of the protection group as a whole to provide the protection switching function properly and to send a notification when a change in its operational state occurs.

- Indicate the status of each individual protection unit such as automatic switch completed.

- Send a notification, identifying the protection unit and protection group, when a protection switch event occurs.

- Send a notification when protection resources are added or removed on the NE.

- For each protected or protecting resource, the ability to perform the following management operations:

  d) invoke a manual protection request;

  e) invoke a forced protection switch;

  f) lockout a protection or working channel;

  g) determine the operational state of the protection group;

  h) indicate a resource as protecting or protected (although most but not all 1+1 systems are symmetrical with respect to their protection switching or management functionality). The equipment in the NE determines this operation and provides this indication;

  i) ability to set the switch priority for protected resources in 1:n systems.

- Support scheduled switching (on a time basis) between protected and protecting units inside a protection group.

B.3.2 Management functions

B.3.2.1 Fault management

B.3.2.1.1 Fault correction

B.3.2.1.1.1 General Functional Model

Refer to subclause 4.5.1.3.1 of the present document

B.3.2.1.1.2 TMN Management Functions

1) *Invoke protection* - The Manager requests the Agent to start a protection action (lockout, manual or forced switch). (B,E,G) (ITU-T Recommendation G.774-03 [9])

2) *Release protection* - The Manager requests the Agent to end a protection action releasing the protecting units. (B,E,G) (ITU-T Recommendation G.774-03 [9])

3) *Protection action reporting* - The Agent notifies the Manager for any protection action that has taken place in the NE. (B,E,G) (ITU-T Recommendation G.774-03 [9])

4) *State change reporting* - The Agent reports any stateChange connected to equipment protection. (B,E,G) (ITU-T Recommendation X.721 [21])

B.3.2.2 Configuration management

B.3.2.2.1 Provisioning

The following paragraphs are equivalent to subclause 4.5.2.2.3 of the present document.

B.3.2.2.1.1 Equipment Protection

B.3.2.2.1.1.1 General Functional Model

Equipment protection is concerned with the provision of protection functions to physical or administrative resources in a NE. The basic administrative resource that allows equipment protection management is the protection group. A protection group object contains zero or more protection unit objects which represent the protected and protecting resources (administrative or physical). The properties of a protection group may be defined according to protection architectures (1+1 or m:n, revertive or non-revertive, specification of a wait-to-restore time). The protection unit object is associated with the resource that is to be protected or with the protecting resource.

Actions may be invoked to request a lockout, a forced switch or a manual switch on a protected unit. The protecting unit that is activated may be released via a lockout, forced switch or manual switch release action. The protection switch reports every protection action via a protection switch report.

The OS may change the configuration of a protection group (1+1 or m:n, revertive or non-revertive, wait-to-restore time) via management operations. The OS may change the priority attribute of a protection unit to set priorities in the case of multiple protection requests.

B.3.2.2.2.1.2 TMN Management Functions

1) *Establish protection* - The Manager instructs the Agent to create a protection scheme. (H) (ETSI RE/TM 2213-1 [7])

2) *Modify protection* - The Manager requests the Agent to modify a protection scheme. (H) (ETSI RE/TM 2213-1 [7])

3) *Dismiss protection* - The Manager instructs the Agent to dismiss a protection scheme. (H) (ETSI RE/TM 2213-1 [7])

4) *Set protection group characteristics* - The Manager configures the protection group characteristics at the Agent. (H) (ITU-T Recommendation G.774-03 [9])

5) *Create protection group* - The Manager creates a protection group in the Agent. (H) (ITU-T Recommendation G.774-03 [9])

6) *Delete protection group* - The Manager deletes a protection group in the Agent. (H) (ITU-T Recommendation G.774-03 [9])

7) *State change reporting* - The Agent reports any stateChange connected to equipment protection. (H) (ITU-T Recommendation X.721 [21])

8) *Create/delete reporting* - The agent notifies the creation/deletion of a protection group. (H) (ITU-T Recommendation M.3100 [13])

9) *Attribute value change reporting* - The agent notifies any change in the attributes of a protection group or a protection unit. (H) (ITU-T Recommendation M.3100 [13])

10) *Get/Set priority values* - The Manager determines the priority to be assigned to a protection unit for protection switching requests. (H) (ITU-T Recommendation G.774-03 [9])

11) *Protection action scheduling* - The Manager determines the scheduling of protection actions for proactive maintenance purposes. (H)

B.4 Information model

B.4.1 Inheritance diagram

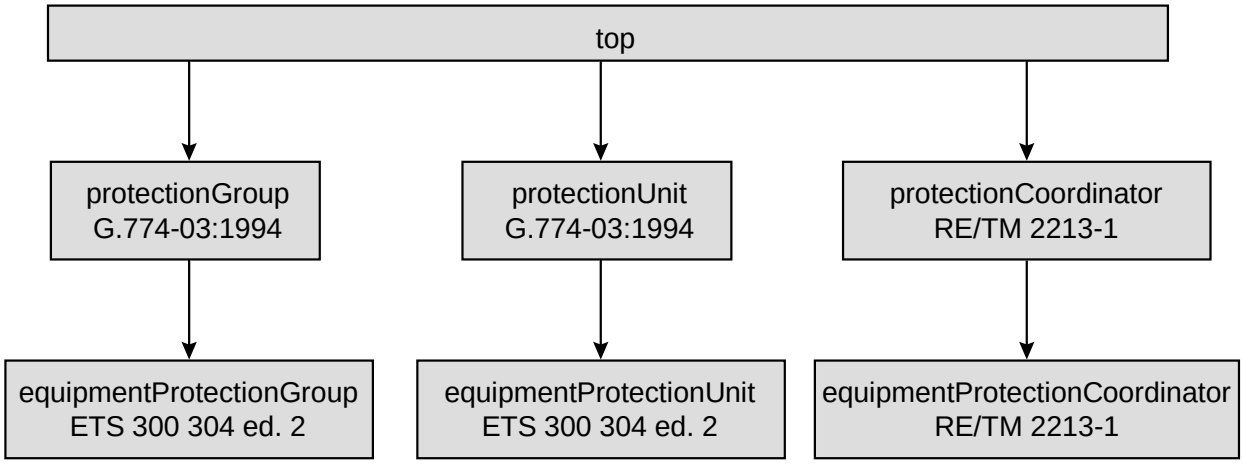

Figure 19: Alternative inheritance diagram for equipment protection.

B.4.2 Containment diagram

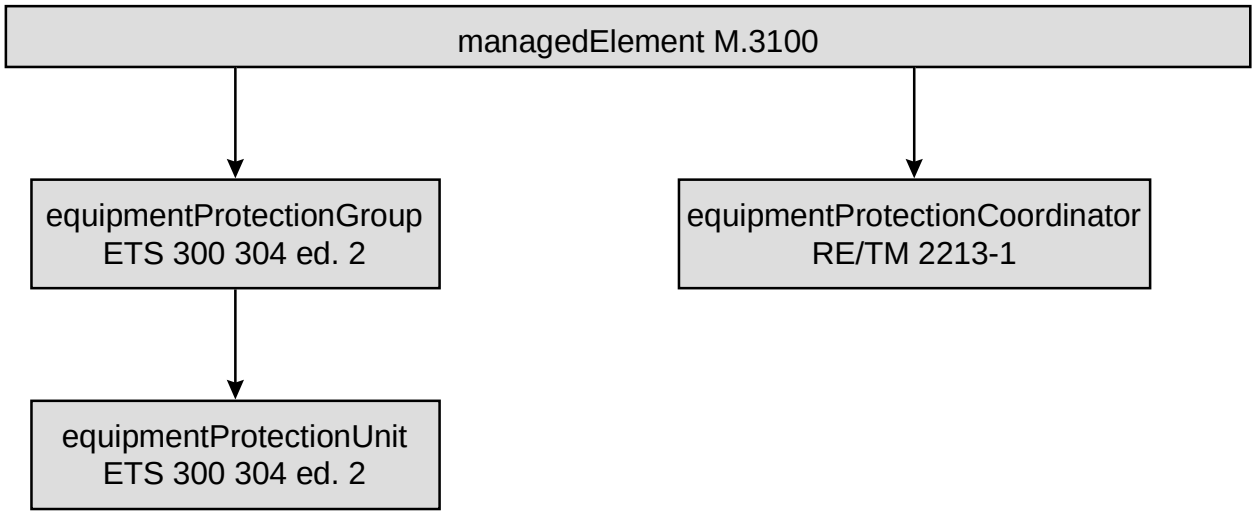

Figure 20: Alternative containment diagram for equipment protection.

B.4.3 Support fragment

B.4.3.1 Managed object class definitions

The managed object classes imported in this subclause replace the change over function managed object classes (ITU-T Recommendation X.751 [20]) imported in subclause 5.6 of the present document.

The following managed object classes are imported from ETS 300 304-2 [6]:

- equipmentProtectionGroup
- equipmentProtectionUnit

The following managed object classes are imported from (ETSI RE/TM 2213-1 [7]):

- equipmentProtectionCoordinator
- syncProtectionGroup
- syncProtectionUnit

Annex C (informative): Commonly used terminology for redundancy schemes

C.1 Background

Redundancy schemes often are commonly identified by using different terminologies, which often derive from technology specific use. This informative annex is intended to give guidance throughout the different terms that were identified during the development of the present document. The following clauses are not intended to be exhaustive.

C.2 Terminology

Table 5 contains a comparison of three different terminolgies that are currently in use in different fields of application (namely SDH, OSI systems management, generic terminology). Each column in the table identifies a set of terms, while each row identifies equivalent terms pertaining to different terminologies.

Table 5: Comparison of different terminologies for redundancy schemes

OSI Systems Management	SDH	Generic
Hot Standby	1+1	Hot Standby
Cold Standby	1:1	Cold Standby or 1+1
Cold Standby	1:n	Cold Standby or N+1
Cold Standby	m:n	Cold Standby or N+K

History

Document history		
Date	**Status**	**Comment**
V1.1.1	October 1997	MAP MV 9751: 1997-10-21 to 1997-12-19