

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3703

(06/2010)

SERIES M: TELECOMMUNICATION MANAGEMENT,
INCLUDING TMN AND NETWORK MAINTENANCE

Integrated services digital networks

Common management services – Alarm management – Protocol neutral requirements and analysis

Recommendation ITU-T M.3703



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	M.3000–M.3599
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

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



Recommendation ITU-T M.3703

Common management services – Alarm management – Protocol neutral requirements and analysis

Summary

Recommendation ITU-T M.3703 provides the requirements and analysis for one of the common management services – alarm management. The functional requirements for the alarm management interface include the management functions for alarm forwarding and filtering, clearing of alarms, storage and retrieval of alarms in/from the agent, configuration of alarms, alarm acknowledgement and alarm notification failure. In the analysis part, the detailed information model supporting the above functions across the management interface is provided.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T M.3703	2010-06-29	2

Keywords

Agent, alarm management, analysis, fault management, interface, manager, requirements.

FOREWORD

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

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

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

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2011

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations.....	2
5	Conventions	3
6	Requirements	3
	6.1 Concepts and background.....	3
	6.2 Business-level requirements	3
	6.3 Specification-level requirements	7
7	Analysis	15
	7.1 Concepts and background.....	15
	7.2 Information object classes	16
	7.3 Interface definition	29
	Annex A – Event Types	53
	Annex B – Probable Causes.....	54
	Appendix I – Examples of using notifyChangedAlarm.....	63
	Appendix II – Background information about fault management	65
	II.1 Fault detection	65
	II.2 Alarm acknowledgement.....	66
	II.3 Clearing of alarms	66
	II.4 Fault recovery	67
	Bibliography.....	69

Introduction

A network is composed of a multitude of network elements (NE) of various types and, typically, different vendors, which interoperate in a coordinated manner in order to satisfy the network users' communication requirements.

The occurrence of failures in a NE may cause a deterioration of this NE's function and/or service quality and will, in severe cases, lead to the complete unavailability of the respective NE. In order to minimize the effects of such failures on the quality of service (QoS) as perceived by the network users, it is necessary to:

- detect failures in the network as soon as they occur and alert the operating personnel as fast as possible;
- isolate the failures (autonomously or through operator intervention), i.e., switch off faulty units and, if applicable, limit the effect of the failure as much as possible by reconfiguration of the faulty NE/adjacent NEs;
- if necessary, determine the cause of the failure using diagnosis and test routines; and
- repair/eliminate failures in due time through the application of maintenance procedures.

This aspect of the management environment is termed "fault management" (FM). The purpose of FM is to detect failures as soon as they occur and to limit their effects on the network quality of service (QoS) as far as possible.

The latter is achieved by bringing additional/redundant equipment into operation, reconfiguring existing equipment/NEs, or by repairing/eliminating the cause of the failure. Degradation of service may be detected by monitoring error rates. Threshold mechanisms on counters and gauges are a method of detecting such trends and providing a warning to managers when the rate becomes high.

Alarms are a specific type of notification concerning detected faults or abnormal conditions. Managed object definers are encouraged to include in alarms information that will help understand the cause of the potentially abnormal situation, and other information related to side effects. An example of such diagnostic information is the current and past values of the configuration management state of the object.

A single incident may cause the generation of several notifications; it is important to be able to specify in a notification some correlation with other notifications. However, the mechanism, if any, for determining the relationship between notifications resulting from a single incident is for further study.

The functional areas specified in this Recommendation cover:

- notification of alarms (including alarm cease) and operational state changes;
- retrieval of current alarms;
- alarm filtering;
- management of alarm severity levels;
- retention of alarm and operational state data in the NEs and the operations system (OS).

Any (re)configuration activities exerted from the element manager (EM) as a consequence of faults is out of the scope of this Recommendation.

This Recommendation defines the requirements for fault management.

Recommendation ITU-T M.3703

Common management services – Alarm management – Protocol neutral requirements and analysis

1 Scope

This Recommendation defines an interface through which an agent (typically a network element or a network element manager) can communicate alarm information for its managed objects to one or several managers (typically network management systems).

This Recommendation defines the semantics of alarms and the interactions visible across the reference point in a protocol neutral way. It defines the semantics of the operations and notifications visible on the interface. It does not define the syntax or encoding of the operations, notifications and their parameters.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T M.3020] Recommendation ITU-T M.3020 (2009), *Management interface specification methodology*.
- [ITU-T M.3100] Recommendation ITU-T M.3100 (1995), *Generic network information model*.
- [ITU-T M.3160] Recommendation ITU-T M.3160 (2008), *Generic, protocol-neutral management information model*.
- [ITU-T M.3702] Recommendation ITU-T M.3702 (2010), *Common management services – Notification management – Protocol neutral requirement and analysis*.
- [ITU-T X.701] Recommendation ITU-T X.701 (1997) | ISO/IEC 10040:1998, *Information technology – Open Systems Interconnection – Systems management overview*.
- [ITU-T X.721] Recommendation ITU-T X.721 (1992) | ISO/IEC 10165-2:1992, *Information technology – Open Systems Interconnection – Structure of management information: Definition of management information*.
- [ITU-T X.733] Recommendation ITU-T X.733 (1992) | ISO/IEC 10164-4:1992, *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*.
- [ITU-T X.736] Recommendation ITU-T X.736 (1992) | ISO/IEC 10164-7:1992, *Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function*.
- [ITU-T X.790] Recommendation ITU-T X.790 (1995), *Trouble management function for ITU-T applications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 alarm [ITU-T X.733].

3.1.2 agent [ITU-T M.3020].

3.1.3 event [ITU-T X.790].

3.1.4 error [ITU-T X.733].

3.1.5 fault [ITU-T X.733].

3.1.6 manager [ITU-T M.3020].

3.1.7 notification [ITU-T X.701].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 active alarm: An alarm that has not been cleared and which is active until the fault that caused the alarm is corrected and a "clear alarm" is generated.

3.2.2 ADAC faults: Faults that are automatically detected and automatically cleared by the system when they occur and when they are repaired.

3.2.3 ADMC faults: Faults that are automatically detected by the system when they occur and manually cleared by the operator when they are repaired.

3.2.4 alarm notification: Notification used to inform the recipient about the occurrence of an alarm.

3.2.5 clear alarm: Notification used to inform the recipient about the cessation of an alarm and thus the underlying fault condition.

4 Abbreviations

This Recommendation uses the following abbreviations:

ADAC Automatically Detected and Automatically Cleared

ADMC Automatically Detected and Manually Cleared

ASAP Alarm Severity Assignment Profile

CO Conditional-Optional

DN Domain Name

EM Element Manager

FM Fault Management

FS Function Set

IOC Information Object Class

M Mandatory

MO Managed Object

MOC Managed Object Class

MOI Managed Object Instance

NE	Network Element
NM	Network Manager
O	Optional
OS	Operations System
QoS	Quality of Service

5 Conventions

This Recommendation uses the conventions defined in [ITU-T M.3020] for requirements capture and analysis.

6 Requirements

6.1 Concepts and background

Any evaluation of the NEs' and the overall network health status requires the detection of faults in the network and, consequently, the notification of alarms to the OS (EM and/or NM). Depending on the nature of the fault, it may be combined with a change of the operational state of the logical and/or physical resource(s) affected by the fault. Detection and notification of these state changes is as essential as it is for the alarms. A list of active alarms in the network and operational state information as well as alarm/state history data may be required by the system operator for further analysis. Additionally, test procedures may be used in order to obtain more detailed information if necessary, or to verify an alarm, a state or the proper operation of NEs and their logical and physical resources.

This service uses the following other services and thus implicitly imports all the requirements defined therein:

- Notification, defined in [ITU-T M.3702].

6.2 Business-level requirements

Faults that may occur in the network can be grouped into one of the following categories:

- Hardware failures, i.e., the malfunction of a physical resource within a NE.
- Software problems, e.g., software bugs, database inconsistencies.
- Functional faults, i.e., a failure of a functional resource in a NE and no hardware component can be found responsible for the problem.
- Loss of some or all of the NE's specified capability due to overload situations.
- Communication failures between two NEs, or between NE and OS, or between two OSs.

6.2.1 Requirements

6.2.1.1 Alarm forwarding and filtering

REQ-FM-FUN-01 For each detected fault, the agent shall generate appropriate alarms (notifications of the fault), regardless of whether it is an ADAC or an ADMC fault. Each alarm should be uniquely identified. For each alarm, the agent shall supply the following information:

- the managed entity;
- the device/resource/file/functionality/smallest replaceable unit as follows:
 - for hardware faults, the smallest replaceable unit that is faulty;

- for software faults, the affected software component, e.g., corrupted file(s) or databases or software code;
- for functional faults, the affected functionality;
- for faults caused by overload, information on the reason for the overload;
- for all the above faults, wherever applicable, an indication of the physical and logical resources that are affected by the fault and a description of the loss of capability of the affected resource;
- the type of the fault (communication, environmental, equipment, processing error, QoS, security types, etc.);
- the severity of the fault (indeterminate, warning, minor, major, critical);
- the probable cause of the fault;
- the specific problem;
- the time at which the fault was detected;
- the nature of the fault, e.g., ADAC or ADMC; any other information that helps understanding the cause and the location of the abnormal situation (system/implementation specific).

REQ-FM-FUN-02 The manager shall be able to allow or suppress alarm reporting by setting the filtering on any combination of attributes. The following criteria shall minimally be supported for alarm notification filtering:

- the managed entity that generated the alarm, i.e., all alarm messages for that managed entity shall be suppressed;
- the device/resource/function to which the alarm relates;
- the severity of the alarm;
- the time at which the alarm was detected, i.e., the alarm time.

6.2.1.2 Clearing of alarms

REQ-FM-FUN-03 Each time an alarm is cleared, the agent shall generate an appropriate clear alarm event. A clear alarm is defined as an alarm. A clear alarm is identified as such through the use of perceived severity equal to CLEARED.

REQ-FM-FUN-04 The manager may explicitly request the clearing of one or more alarms. Once the alarm(s) has/have been cleared, the agent should reissue those alarms (as new alarms) in case the fault situation still persists.

6.2.1.3 Storage and retrieval of alarms in/from the agent

REQ-FM-FUN-05 The manager shall be able to retrieve alarm information optionally using filters (active and/or historic).

6.2.1.4 Configuration of ASAP

REQ-FM-FUN-06 It may be possible for the manager to create an ASAP on an agent to define the relationship between severity level and problem.

REQ-FM-FUN-07 It may be possible for the manager to modify the ASAP.

REQ-FM-FUN-08 It may be possible for the manager to delete the ASAP on an agent.

REQ-FM-FUN-09 It may be possible for the manager to request an agent to set or change the association between an ASAP and one or more specified managed entities.

REQ-FM-FUN-10 It may be possible for the manager to request an agent to remove the association between an ASAP and one or more of its associated managed entities.

REQ-FM-FUN-11 The manager may query the attribute information of an ASAP, which includes the ID of the ASAP, the list of the problem and the corresponding severity, and the list of managed entities that have been associated with this ASAP.

6.2.1.5 Alarm acknowledgement and management

REQ-FM-FUN-12 An agent may support alarm acknowledgement and unacknowledgement. Acknowledgement data shall include the current alarm state (active|cleared), the time of alarm acknowledgement and, optionally, the system (EM|NM) or the operator in charge of acknowledgement (the parameter operator name or, in case of auto-acknowledgement, a generic system name).

REQ-FM-FUN-13 An alarm acknowledgement means that an acknowledgement performed by the agent is notified to the manager and vice versa, thus the acknowledgement-related status of this alarm is the same across the whole management hierarchy.

REQ-FM-FUN-14 The agent may provide the ability to add a comment to an alarm. An agent may also have the capability to record more than one comment for each alarm. To make the same alarm look the same to all managers subscribing to the alarm, it will be possible to distribute the recorded comments.

REQ-FM-FUN-15 Acknowledgement state shall be a filterable criteria for alarms if acknowledgement is supported by the agent.

REQ-FM-FUN-16 Acknowledgement notifications shall be filtered with the same criteria applied to alarms.

6.2.1.6 Alarm notification failure

REQ-FM-FUN-17 The manager should be able to request an agent to synchronize alarm information following a failure in communication between the agent and the manager.

6.2.2 Actor roles

The capabilities described in this Recommendation are available and relevant to all agents and managers.

6.2.3 Telecommunication resources

The alarm management functionality is applicable to all types of telecommunication resources.

6.2.4 High-level use-case diagrams

The first overview use-case diagram in Figure 6-1 shows the overall interaction of the alarm interface.

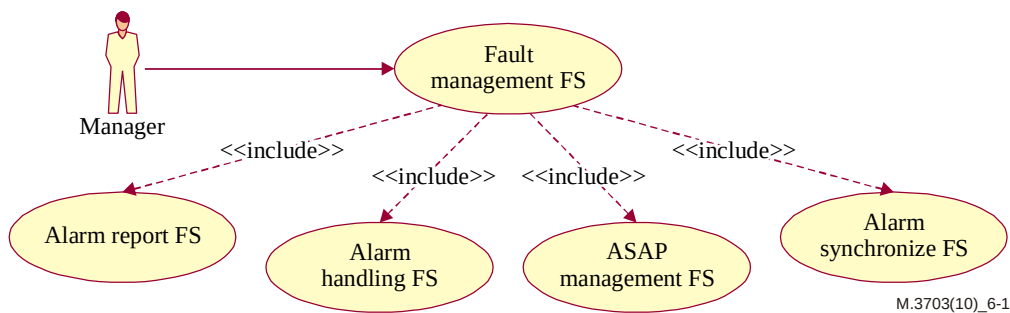


Figure 6-1 – Fault management function set

Figure 6-2 shows the functions involved in the alarm report function set.

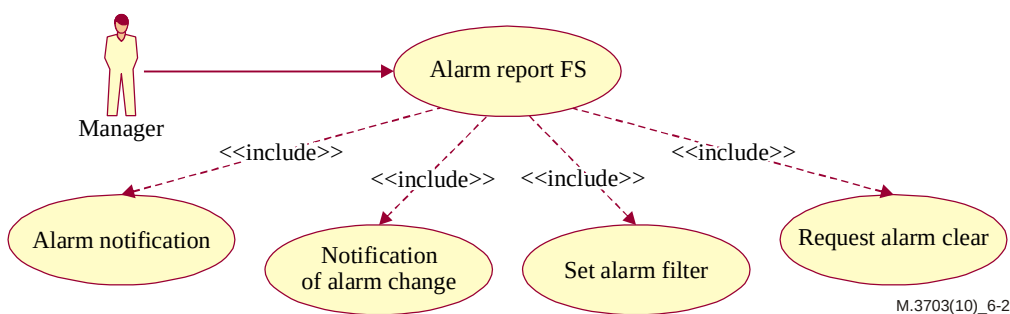


Figure 6-2 – Alarm report function set

Figure 6-3 shows the functions involved in the alarm handling function set.

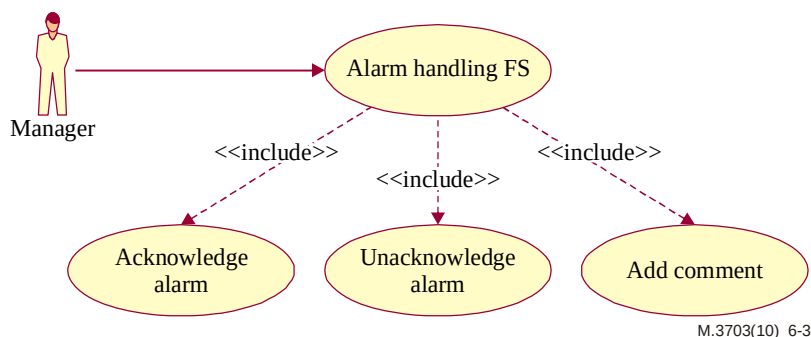


Figure 6-3 – Alarm handling function set

Figure 6-4 shows the functions involved in the ASAP management function set.

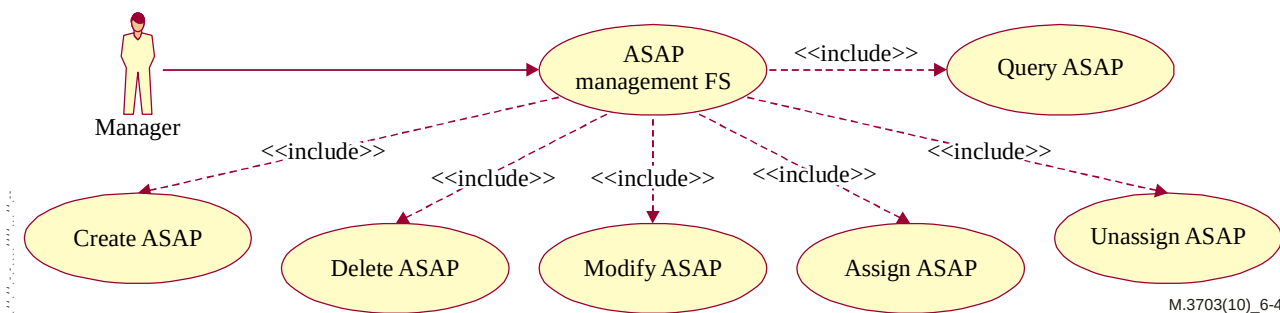


Figure 6-4 – ASAP management function set

Figure 6-5 shows the functions involved in the alarm synchronize function set.

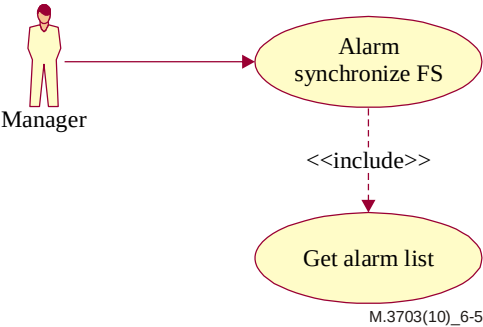


Figure 6-5 – Alarm synchronize function set

6.3 Specification-level requirements

6.3.1 Requirements

There are no specification-level requirements.

6.3.2 Actor roles

See clause 6.2.2.

6.3.3 Telecommunication resources

See clause 6.2.3.

6.3.4 Use cases

6.3.4.1 Use case: Set alarm filter

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager sets a filter for alarm notification subscription.	
Actor and roles	The manager invokes the operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	None.	
Begins when	The manager requests to set a filter to the agent.	
Step 1	The manager requests to set a filter to subscribe alarm information; the manager provides the criteria parameters (e.g., the managed entities, severity level, event type, acknowledgement state, etc.) in the request.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	Invalid parameters.	
Post conditions	The filter is received by the agent.	
Traceability	REQ-FM-FUN-02, REQ-FM-FUN-15	

6.3.4.2 Use case: Alarm notification

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	An agent sends an alarm report notification of the relevant type to the manager.	
Actor and roles	The manager is a consumer of notifications from the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	A fault condition is detected.	
Begins when	The agent begins to send an alarm report notification to the manager.	
Step 1	The agent sends notification of fault and gives parameters (e.g., identifier of alarm, time, severity level, event type, etc.) in the notification.	
Ends when	The notification is emitted by the agent.	
Exceptions	None.	
Post conditions	The manager is informed of the fault condition in the agent.	
Traceability	REQ-FM-FUN-01, REQ-FM-FUN-03	

6.3.4.3 Use case: Notification of alarm change

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	An agent notifies the subscribed manager of the information change of an alarm.	
Actor and roles	The manager is a consumer of notifications from the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The information (e.g., state, comment, etc.) of an alarm is changed.	
Begins when	The agent begins to send a notification to the subscribed managers.	
Step 1	When the agent notifies the managers of the change of information of an alarm, the agent will give some parameters (e.g., identifier of alarm, the new state/status value, the new comment, etc.) as part of the notification.	
Ends when	The notification is emitted by the agent.	
Exceptions	None.	
Post conditions	The manager is informed of the change of an alarm.	
Traceability	REQ-FM-FUN-09, REQ-FM-FUN-10	

6.3.4.4 Use case: Request alarm clear

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager explicitly requests the clearing of one or more alarms.	
Actor and roles	The manager invokes the operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The alarm to be cleared exists.	
Begins when	The manager begins to request clearing of one or more alarms.	
Step 1	The manager sends a request to the agent to clear one or more alarms, the parameters given in the request can be identifier of alarm, severity level and other parameters.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	Invalid parameters.	
Post conditions	The specified alarms are cleared and the agent sends a notification to the subscribed manager.	
Traceability	REQ-FM-FUN-04	

6.3.4.5 Use case: Get alarm list

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager requests and receives a list of alarms from the agent.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The manager sends a request to the agent to get alarm list.	
Begins when	The manager requests active alarm list from an agent with a filtering criteria.	
Step 1	A list of alarms, starting at the oldest, according to the filtering criteria, is received by the manager.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	Invalid criteria parameter.	
Post conditions	The complete list of alarms (active and/or historic) at the time of the initial request is received by the manager.	
Traceability	REQ-FM-FUN-05, REQ-FM-FUN-17	

6.3.4.6 Use case: Acknowledge alarm

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager requests an alarm to be acknowledged.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available. The agent supports the acknowledged state alarm attribute.	
Preconditions	The specified alarm has not been acknowledged.	
Begins when	The manager requests an alarm to be marked as acknowledged.	
Step 1	The manager sends a request to the agent to set the acknowledged state of an alarm to TRUE.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– unknown alarm; – the alarm has been already acknowledged.	
Post conditions	The agent marks the alarm as acknowledged, and the agent sends a notification of the event to the subscribed managers.	
Traceability	REQ-FM-FUN-12, REQ-FM-FUN-13, REQ-FM-FUN-16	

6.3.4.7 Use case: Unacknowledge alarm

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager requests that an acknowledged alarm be unacknowledged.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available. The agent supports the acknowledged state alarm attribute.	
Preconditions	The specified alarm has been acknowledged.	
Begins when	The manager requests an alarm be marked as not acknowledged.	
Step 1	The manager sends a request to the agent to set the acknowledged state of an alarm to FALSE.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– unknown alarm; – the alarm has not been acknowledged.	
Post conditions	The agent marks the alarm as not acknowledged, and the agent sends a notification of the event to the subscribed managers.	
Traceability	REQ-FM-FUN-12, REQ-FM-FUN-13, REQ-FM-FUN-16	

6.3.4.8 Use case: Create ASAP

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	A manager requests an agent to create an ASAP through the management interface.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The manager needs to assign the alarm severities for a set of problems, so that when an agent reports alarms, these pre-assigned severities can be referenced in the corresponding alarm notifications.	
Begins when	The manager sends a request to the agent to create an ASAP.	
Step 1	The manager requests to create an ASAP, and gives the parameters (problems and their corresponding severity) in the request.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– invalid parameter; – unknown managed entity.	
Post conditions	An ASAP is successfully created by the agent according to the request. The agent returns the identifier of the ASAP instance. The newly created ASAP will be associated with the managed entities, if specified in the request.	
Traceability	REQ-FM-FUN-06	

6.3.4.9 Use case: Delete ASAP

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	A manager requests an agent to delete an ASAP through the management interface.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The specified ASAP exists in the agent, and it is not associated with any managed entities.	
Begins when	The manager sends a request to the agent to delete an ASAP.	
Step 1	The manager sends a request to the agent to delete an ASAP. The request parameter is the identifier of the ASAP. The ASAP to be deleted should not be associated with any managed object; otherwise it cannot be deleted. If the deletion operation succeeds, the agent returns a success indication, and may send an object deletion notification to the manager.	



Use case stage	Evolution/Specification	<<Uses>> Related use
	If the operation fails, the agent will send back error information to the manager.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– unknown ASAP; – ASAP association not removed.	
Post conditions	The ASAP is successfully deleted by the agent according to the request.	
Traceability	REQ-FM-FUN-08	

6.3.4.10 Use case: Modify ASAP

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	A manager requests an agent to modify, add or delete table entries (problem and the corresponding alarm severity) of an ASAP.	
Actor and roles	The manager invokes operation on the agent.	
Assumptions	The communication between the manager and the agent is available.	
Telecom resources	All types of telecommunication resources.	
Preconditions	The manager needs to change the table entries of the alarm severity assignment of an ASAP.	
Begins when	The manager sends a request to an agent to modify an ASAP.	
Step 1	The manager sends a request to the agent to modify an ASAP. The request parameter is the new list of the problems and their corresponding severity to be modified. If the modification operation succeeds, the agent will send success information. If the operation fails, the agent will send back error information to the manager.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– unknown ASAP; – invalid parameter.	
Post conditions	An ASAP on the agent is successfully modified according to the request.	
Traceability	REQ-FM-FUN-07	

6.3.4.11 Use case: Assign ASAP

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	A manager requests an agent to set or change the association between an ASAP instance and one or more specified managed entities.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The specified ASAP exists in the agent.	
Begins when	The manager sends a request to the agent to change the association between an ASAP instance and one or more specified managed entities.	
Step 1	When an ASAP is created successfully, it will not take effect immediately until associated with managed entities. When a managed entity is about to report an alarm, it will first check in the associated ASAP whether the corresponding alarm severity is specified. If already specified, the corresponding severity is assigned to the alarm and then it is reported to the manager. Otherwise, the original severity is applied. In this use case, the manager sends a request to the agent to set or change the ASAP association. The request parameter is the ID or a list of IDs of the managed entities to be associated with the ASAP. If the operation succeeds, the agent will return success information, and the ASAP starts to take effect on the specified managed entity(s). If the operation fails, the agent will return error information.	
Ends when	Requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– unknown managed entity; – unknown ASAP.	
Post conditions	The association between the ASAP and the specified managed entity(s) is successfully assigned by the agent. The ASAP then takes effect on the associated managed entity(s).	
Traceability	REQ-FM-FUN-09	

6.3.4.12 Use case: Unassign ASAP

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	A manager removes the association between an ASAP and some of its associated managed entity(s).	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	

Use case stage	Evolution/Specification	<<Uses>> Related use
Preconditions	The specified ASAP exists in agent. The association between the ASAP and the specified managed entity(s) has been assigned. The manager does not want the specified managed entity(s) to refer to this ASAP.	
Begins when	The manager sends a request to the agent to remove the association between an ASAP and some of its associated managed entity(s).	
Step 1	When an ASAP is associated with a managed object, it starts to take effect. When the association between an ASAP and a managed element is no longer needed, it can be removed. If the manager wants to associate a managed object with another ASAP, the association with the previous ASAP must be removed first. In this use case, the manager sends a remove ASAP association request to the agent. The request parameter is: the ID or list of IDs of the managed entity(s) associated with the ASAP. If the operation succeeds, the agent will return success information, and the ASAP associated with specified managed object(s) will not take effect any longer. If the operation fails, the agent will return error information to the manager.	
Ends when	The requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– unknown managed entity; – the association does not exist.	
Post conditions	The association between the ASAP and the specified managed object(s) is removed by the agent. The agent may send the related attribute value change notifications to the manager.	
Traceability	REQ-FM-FUN-10	

6.3.4.13 Use case: Query ASAP

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	A manager queries the information of an ASAP through the management interface.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available.	
Preconditions	The specified ASAP exists in the agent.	
Begins when	The manager sends a request to query the information of an ASAP.	
Step 1	The manager sends a request to the agent to query the attribute information of an ASAP, which includes the ID of the ASAP, the list of the problem and the corresponding severity, and the list of managed entities that have been associated with this ASAP.	

Use case stage	Evolution/Specification	<<Uses>> Related use
	If the operation succeeds, the agent will return the corresponding attribute values of the ASAP. If the operation fails, the agent will return error information.	
Ends when	The requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	None.	
Post conditions	The corresponding ASAP information is returned by the agent.	
Traceability	REQ-FM-FUN-11	

6.3.4.14 Use case: Add Comment

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager requests that a comment be added to the attributes of an alarm.	
Actor and roles	The manager invokes operation on the agent.	
Telecom resources	All types of telecommunication resources.	
Assumptions	The communication between the manager and the agent is available. The agent supports an operation of adding comment.	
Preconditions	The alarm exists.	
Begins when	The manager requests a comment be added to an alarm.	
Step 1	The manager sends a request to the agent to add a comment to an alarm, which includes the date and time of the annotation, the text of the comment, the userid, and the identifier of the manager.	
Ends when	The requested information or an exception is returned to the manager, or the operation is cancelled by the manager.	
Exceptions	– invalid alarm identifier; – invalid parameters.	
Post conditions	The agent adds the comment to the specified alarms and sends a notification of the event to subscribed managers.	
Traceability	REQ-FM-FUN-14	

7 Analysis

7.1 Concepts and background

The alarm management service makes use of the common management services shown in Figures 7-1 and 7-2.

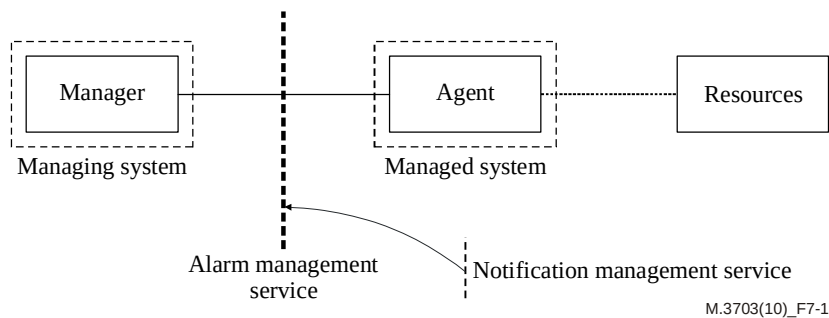


Figure 7-1 – System context A

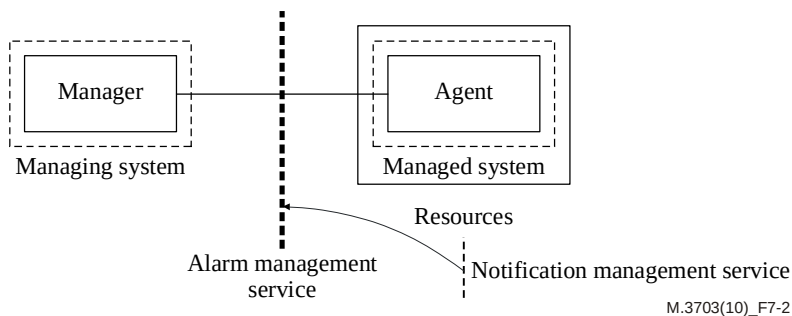


Figure 7-2 – System context B

7.2 Information object classes

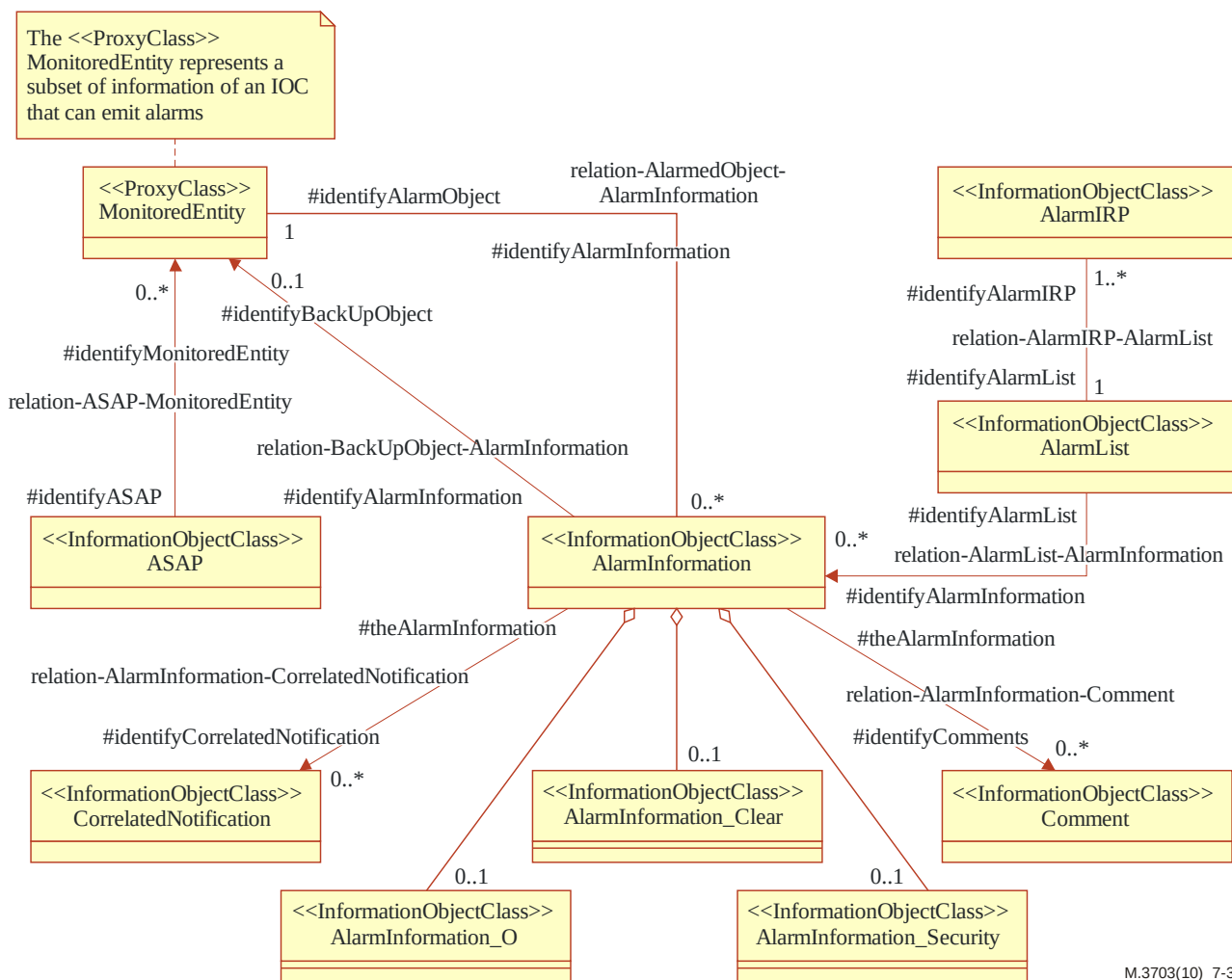
7.2.1 Imported information entities and local label

Label reference	Local label
[ITU-T M.3702], information object class, NotificationIRP	NotificationIRP
[ITU-T M.3160], information object class, Top	Top

7.2.2 Class diagram

This clause introduces the set of information object classes (IOCs) that encapsulate information within the agent. The intent is to identify the information required for the alarm agent implementation of its operations and notification emission. This clause provides the overview of all support object classes in UML. Subsequent clauses provide more detailed specification of various aspects of these support object classes.

7.2.2.1 Attributes and relationships



M.3703(10)_7-3

Figure 7-3 – Alarm management information object classes

7.2.2.2 Inheritance

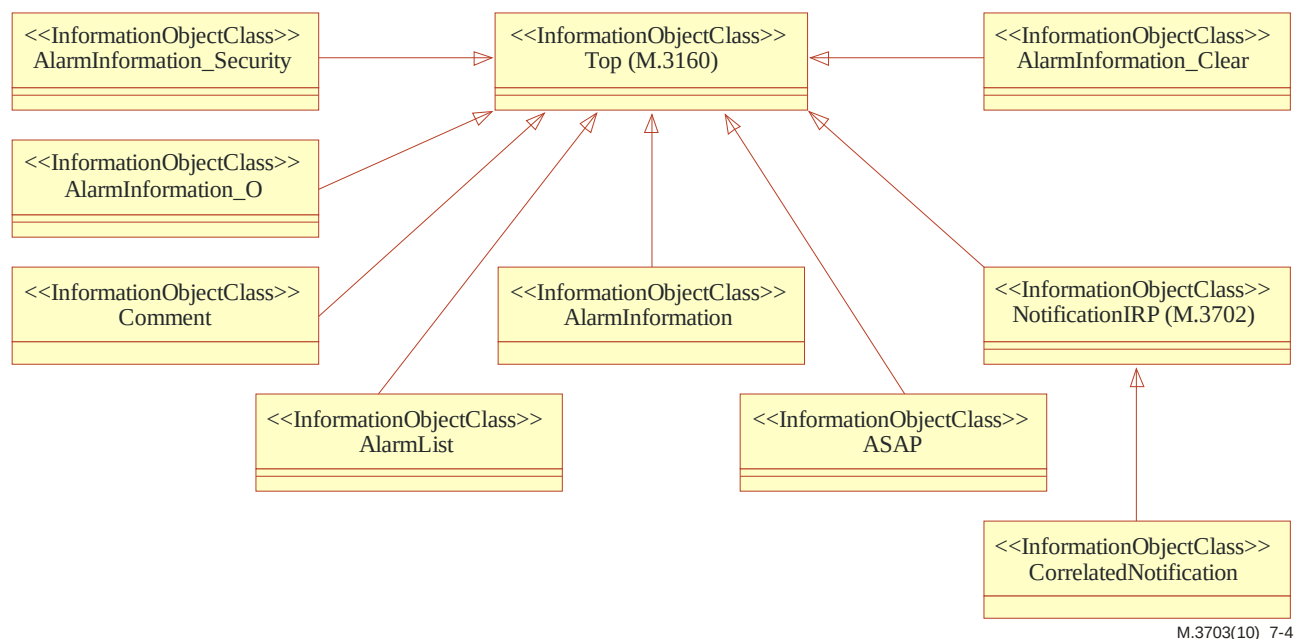


Figure 7-4 – Alarm management IOC inheritance

7.2.3 Information object class definitions

Class name	Qualifier	Requirement IDs
AlarmInformation	M	REQ-FM-FUN-01, REQ-FM-FUN-02, REQ-FM-FUN-03, REQ-FM-FUN-12
AlarmInformation_O	O	REQ-FM-FUN-01, REQ-FM-FUN-02, REQ-FM-FUN-03, REQ-FM-FUN-12
AlarmInformation_Clear	CO (see Note 1)	REQ-FM-FUN-04
AlarmInformation_Security	CO (see Note 2)	REQ-FM-FUN-01
AlarmList	M	REQ-FM-FUN-05, REQ-FM-FUN-17
Comment	M	REQ-FM-FUN-14
CorrelatedNotification	M	REQ-FM-FUN-01
ASAP	O	REQ-FM-FUN-06, REQ-FM-FUN-07, REQ-FM-FUN-08, REQ-FM-FUN-09, REQ-FM-FUN-10, REQ-FM-FUN-11
AlarmIRP	M	REQ-FM-FUN-01, REQ-FM-FUN-05, REQ-FM-FUN-17

NOTE 1 – These attributes and qualifiers are applicable only if the agent supports clearAlarms() (they are absent if clearAlarms() is not supported).

NOTE 2 – These attributes must be supported if the agent emits NewAlarmNotification that carries security alarm information.

7.2.3.1 AlarmInformation

7.2.3.1.1 Definition

AlarmInformation contains information about the alarm condition of an alarmed MonitoredEntity.