INTERNATIONAL STANDARD

ISO/IEC 10164-4

First edition
1992-12-15

Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function

Technologies de l'information – Interconnexion de systèmes ouverts – Gestion-système: Fonction de compte rendu d'alarme

Reference number
ISO/IEC 10164-4:1992 (E)

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO 10164-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with the CCITT. The identical text is published as CCITT Recommendation X.733.

ISO/IEC 10164 consists of the following parts, under the general title *Information technology – Open Systems Interconnection – Systems Management*:

- *Part 1: Object management function*
- *Part 2: State management function*
- *Part 3: Attributes for representing relationships*
- *Part 4: Alarm reporting function*
- *Part 5: Event report management function*
- *Part 6: Log control function*
- *Part 7: Security alarm reporting function*
- *Part 8: Security audit trail function*
- *Part 9: Objects and attributes for access control*
- *Part 10: Accounting meter function*
- *Part 11: Workload monitoring function*
- *Part 12: Test management function*
- *Part 13: Summarization function*
- *Part 14: Confidence and diagnostic test categories*

Introduction

ISO/IEC 10164 is a multipart standard developed according to ISO 7498 and ISO/IEC 7498-4. ISO/IEC 10164 is related to the following International Standards:

— ISO/IEC 9595 : 1990, *Information technology - Open Systems Interconnection - Common management information service definition*;

— ISO/IEC 9596 : 1990, *Information technology - Open Systems Interconnection - Common management information protocol*;

— ISO/IEC 10040 : 1992, *Information technology - Open Systems Interconnection - Systems management overview*;

— ISO/IEC 10165 : 1992, *Information technology - Open Systems Interconnection - Structure of management information.*

This page intentionally left blank

INTERNATIONAL STANDARD

CCITT RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: ALARM REPORTING FUNCTION

1 Scope

This Recommendation | International Standard defines a Systems Management Function that may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management, as defined by CCITT Rec. X.700 | ISO/IEC 7498-4. This Recommendation | International Standard defines a function which consists of generic definitions, services and functional units. This function is positioned in the application layer of the OSI reference model (CCITT Rec. X.200 | ISO 7498) and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040. The alarm notifications defined by this function provides information that a manager may need to act upon pertaining to a system's operational condition and quality of service.

This Recommendation | International Standard

- establishes user requirements for the alarm reporting function;
- establishes a model that relates the service and generic definitions provided by this function to user requirements;
- defines the service provided by the function;
- defines generic notification types and parameters documented in accordance with CCITT Rec. X.722 | ISO/IEC 10165-4;
- specifies the protocol that is necessary in order to provide the service;
- specifies the abstract syntax necessary to identify and negotiate the functional unit in protocol;
- defines the relationship between this service and SMI notifications;
- specifies compliance requirements placed on other standards that make use of these generic definitions;
- defines relationships with other systems management functions;
- specifies conformance requirements.

This Recommendation | International Standard does not

- define the nature of any implementation intended to provide the Alarm Reporting function;
- specify the manner in which management is accomplished by the user of the Alarm Reporting function;
- define the nature of any interactions which result in the use of the Alarm Reporting function;
- specify the services necessary for the establishment, normal and abnormal release of a management association;
- preclude the definition of further notification types;
- define managed objects.

2 Normative references

The following CCITT Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards. The CCITT Secretariat maintains a list of the currently valid CCITT Recommendations.

2.1 Identical CCITT Recommendations | International Standards

- CCITT Recommendation X.701 (1992) | ISO/IEC 10040 : 1992, *Information technology – Open Systems Interconnection – Systems management overview.*
- CCITT Recommendation X.731 (1992) | ISO/IEC 10164-2 : 1992, *Information technology – Open Systems Interconnection – Systems Management – State management function.*
- CCITT Recommendation X.732 (1992) | ISO/IEC 10164-3 : 1992, *Information technology – Open Systems Interconnection – Systems Management – Attributes for representing relationships.*
- CCITT Recommendation X.734[1)] | ISO/IEC 10164-5 : 1992, *Information technology – Open Systems Interconnection – Systems Management – Event report management function.*
- CCITT Recommendation X.720 (1992) | ISO/IEC 10165-1 : 1992, *Information technology – Open Systems Interconnection – Structure of management information – Management information model.*
- CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2 : 1992, *Information technology – Open Systems Interconnection – Structure of management information – Definition of management information.*
- CCITT Recommendation X.722 (1992) | ISO/IEC 10165-4 : 1992, *Information technology – Open Systems Interconnection – Structure of Management Information – Guidelines for the definition of managed objects.*

2.2 Paired CCITT Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.700[1)] , *Management framework for Open systems Interconnection (OSI) for CCITT applications.*

  ISO/IEC 7498-4 : 1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4 : Management framework.*
- CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT Applications.*

  ISO 7498 : 1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*
- CCITT Recommendation X.208 (1988), *Specification of abstract syntax notation one (ASN.1).*

  ISO/IEC 8824 : 1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*
- CCITT Recommendation X.210 (1988), *Reference Model of Open Systems Interconnection (OSI) Layer Service Definition Conventions for CCITT Applications.*

  ISO/TR 8509 : 1987, *Information processing systems – Open Systems Interconnection – Service conventions.*
- CCITT Recommendation X.710 (1991), *Common Management Information Service Definition for CCITT Applications.*

  ISO/IEC 9595 : 1991, *Information technology – Open Systems Interconnection – Common management information service definition.*

---

1) Presently at state of draft Recommendation.

– CCITT Recommendation X.290 (1992), *OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications – General Concepts.*

ISO/IEC 9646-1 : 1991, *Information technology – Open Systems Interconnection conformance testing methodology and framework – Part 1: General concepts.*

2.3 Additional references

– ISO/IEC 9545 : 1989, Information processing systems – Open Systems Interconnection – Application Layer structure.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Basic reference model definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.200 | ISO 7498.

a) open system;

b) systems management.

3.2 Management framework definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.700 | ISO/IEC 7498-4.

managed object

3.3 CMIS definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.710 | ISO/IEC 9595.

attribute

3.4 Systems management overview definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.701 | ISO/IEC 10040.

a) agent;

b) agent role;

c) dependent conformance;

d) general conformance;

e) generic definitions;

f) manager;

g) manager role;

h) notification;

i) systems management application protocol;

j) systems management functional unit.

3.5 Event report management function definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.734 | ISO/IEC 10164-5.

event forwarding discriminator

3.6 OSI conformance testing definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.290 | ISO/IEC 9646-1.

system conformance statement

3.7 Additional definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.7.1 **error**: A deviation of a system from normal operation.

3.7.2 **fault:** The physical or algorithmic cause of a malfunction. Faults manifest themselves as errors.

3.7.3 **alarm**: A notification, of the form defined by this function, of a specific event. An alarm may or may not represent an error.

3.7.4 **alarm report**: A specific type of event report used to convey alarm information.

4 Abbreviations

ASN.1	Abstract Syntax Notation One
CMIS	Common Management Information Service
Conf	Confirm
Ind	Indication
MAPDU	Management Application Protocol Data Unit
Req	Request
Rsp	Response
SMAPM	Systems Management Application Protocol Machine

5 Conventions

This Recommendation | International Standard defines services following the descriptive conventions defined in CCITT Rec. X.210 | ISO/TR 8509. In clause 9, the definition of each service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values

M	the parameter is mandatory
(=)	the value of the parameter is equal to the value of the parameter in the column to the left
U	the use of the parameter is a service-user option.
–	the parameter is not present in the interaction described by the primitive concerned.
C	the parameter is conditional. The condition(s) are defined by the text which describes the parameter.
P	subject to the constraints imposed on the parameter by CCITT Rec. X.710	ISO/IEC 9595.

NOTE – The parameters which are marked "P" in service tables of this Recommendation | International Standard are mapped directly onto the corresponding parameters of the CMIS service primitive, without changing the semantics or syntax of the parameters. The remaining parameters are used to construct an MAPDU.

6 Requirements

The requirements satisfied by this function are the reporting of alarms, errors and related information, in a standard fashion.

7 Model

Early detection of faults before significant effects have been felt by the user is a desirable requirement of communicating systems. Degradation of service may be detected by monitoring of 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.

An important criterion by which failures of communications resources are to be reported is the level to which the fault degrades the quality of the service that was originally requested by (or promised to) the service user. Malfunctions will range in severity from Warning, where there is no impact upon the quality of service offered to the user, to Critical, where it is no longer possible to provide the service requested by (or promised to) the service user. The level of severity can be described generically and criteria specified based upon the level of degradation that the fault causes to the service: Critical, Major, Minor or Warning.

Alarms are specific types of notifications concerning detected faults or abnormal conditions. Managed object definers are encouraged to include in alarms information that will help with understanding 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 outside the scope of this function.

It is considered important in some circumstances to provide alarm reports with a standardized style, using a common set of notification types, with standardized parameters and parameter definitions, independent of particular managed objects. The notification types specified in this function are intended to be generally applicable and can be imported into the definition of any managed object.

Control of notifications, e.g. whether a notification results in an event report, may be accomplished by use of the Event Report management function defined in CCITT Rec. X.734 | ISO/IEC 10164-5.

8 Generic definitions

8.1 Generic notifications

The set of generic notifications, parameters and semantics defined by this Recommendation | International Standard provide the detail for the following general parameters of the M-EVENT-REPORT service as defined by CCITT Rec. X.710 | ISO/IEC 9595

- event type;
- event information;
- event reply.

All notifications are potential entries in a systems management log and this Recommendation | International Standard defines a managed object class for this purpose. CCITT Rec. X.721 | ISO/IEC 10165-2 defines a generic event log record object class from which all entries are derived, the additional information being specified by the event information and event reply parameters.

8.1.1 Event type

This parameter categories the alarm. Five basic categories of alarm are specified. These are

- communications alarm type: An alarm of this type is principally associated with the procedures and/or processes required to convey information from one point to another;
- quality of service alarm type: An alarm of this type is principally associated with a degradation in the quality of a service;
- processing error alarm type: An alarm of this type is principally associated with a software or processing fault;
- equipment alarm type: An alarm of this type is principally associated with an equipment fault;
- environmental alarm type: An alarm of this type is principally associated with a condition relating to an enclosure in which the equipment resides.

8.1.2 Event information

The following parameters constitute the notification specific information.

8.1.2.1 Probable cause

This parameter defines further qualification as to the probable cause of the alarm. Probable cause values for notifications shall be indicated in the behaviour clause of the object class definition. This Recommendation | International Standard defines, for use within the Systems management application context defined in CCITT X.701 | ISO/IEC 10040, standard Probable causes that have wide applicability across managed object classes. These values are registered in CCITT X.721 | ISO/IEC 10165-2. The syntax of standard Probable causes shall be the ASN.1 type object identifier. Additional standard Probable causes, for use within the Systems management application context defined in CCITT X.701 | ISO/IEC 10040, may be added to this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Other Probable causes, for use within the Systems management application context defined in CCITT X.701 | ISO/IEC 10040, may be defined outside of this Recommendation | International Standard and registered using the procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Probable causes may be defined for use outside of the Systems management application context; the syntax of such Probable causes shall be either an ASN.1 object identifier or ASN.1 type integer.

The managed object class definer should choose the most specific Probable cause applicable.

This Recommendation | International Standard defines the following Probable causes

- adapter error;
- application subsystem failure: A failure in an application subsystem has occurred (an application subsystem may include software to support the Session, Presentation or Application layers);
- bandwidth reduced: The available transmission bandwidth has decreased;
- call establishment error: An error occurred while attempting to establish a connection;
- communications protocol error: A communication protocol has been violated;
- communications subsystem failure: A failure in a subsystem that supports communications over telecommunications links, these may be implemented via leased telephone lines, by X.25 networks, token-ring LAN, or otherwise;
- configuration or customization error: A system or device generation or customization parameter has been specified incorrectly, or is inconsistent with the actual configuration;
- congestion: A system or network component has reached its capacity or is approaching it;
- corrupt data: An error has caused data to be incorrect and thus unreliable;
- CPU cycles limit exceeded: A Central Processing Unit has issued an unacceptable number of instructions to accomplish a task;
- dataset or modem error: An internal error has occurred on a dataset or modem;
- degraded signal: The quality or reliability of transmitted data has decreased;
- DTE-DCE interface error: A problem in a DTE-DCE interface, which includes the interface between the DTE and DCE, any protocol used to communicate between the DTE and DCE and information provided by the DCE about the circuit;
- enclosure door open;
- equipment malfunction: An internal machine error has occurred for which no more specific Probable cause has been identified;
- excessive vibration: Vibratory or seismic limits have been exceeded;
- file error: The format of a file (or set of files) is incorrect and thus cannot be used reliably in processing;
- fire detected;
- flood detected;
- framing error: An error in the information that delimits the bit groups within a continuous stream of bits;
- heating/ventilation/cooling system problem;

- humidity unacceptable: The humidity is not within acceptable limits;
- I/O device error: An error has occurred on the I/O device;
- input device error: An error has occurred on the input device;
- LAN error: An error has been detected on a local area network;
- leak detected: A leakage of (non-toxic) fluid or gas has been detected;
- local node transmission error: An error occurred on a communications channel between the local node and an adjacent node;
- loss of frame: An inability to locate the information that delimits the bit grouping within a continuous stream of bits;
- loss of signal: An error condition in which no data is present on a communications circuit or channel;
- material supply exhausted: A supply of needed material has been exhausted;
- multiplexer problem: An error has occurred while multiplexing communications signals;
- out of memory: There is no program-addressable storage available;
- output device error: An error has occurred on the output device;
- performance degraded: Service agreements or service limits are outside of acceptable limits;
- power problem: There is a problem with the power supply for one or more resources;
- pressure unacceptable: A fluid or gas pressure is not within acceptable limits;
- processor problem: An internal machine error has occurred on a Central Processing Unit;
- pump failure: Failure of mechanism that transports a fluid by inducing pressure differentials within the fluid;
- queue size exceeded: The number of items to be processed (configurable or not) has exceeded the maximum allowable;
- receive failure;
- receiver failure;
- remote node transmission error: An error occurred on a communication channel beyond the adjacent node;
- resource at or nearing capacity: The usage of a resource is at or nearing the maximum allowable capacity;
- response time excessive: The elapsed time between the end of an inquiry and beginning of the answer to that inquiry is outside of acceptable limits;
- retransmission rate excessive: The number of repeat transmissions is outside of acceptable limits;
- software error: A software error has occurred for which no more specific Probable cause can be identified;
- software program abnormally terminated: A software program has abnormally terminated due to some unrecoverable error condition;
- software program error: An error has occurred within a software program that has caused incorrect results;
- storage capacity problem: A storage device has very little or no space available to store additional data;
- temperature unacceptable: A temperature is not within acceptable limits;
- threshold crossed: A limit (configurable or not) has been exceeded;
- timing problem: A process that requires timed execution and/or coordination cannot complete, or has completed but cannot be considered reliable;
- toxic leak detected: A leakage of toxic fluid or gas has been detected;
- transmit failure;
- transmitter failure;

- underlying resource unavailable: An entity upon which the reporting object depends has become unavailable;
- version mismatch: There is a conflict in the functionality of versions of two or more communicating entities which may affect any processing involving those entities.

8.1.2.2 Specific problems

This parameter, when present, identifies further refinements to the Probable cause of the alarm. This parameter qualifies the chosen Probable cause and may be used by the managed object class definer to specify a set of identifiers for use in managed object classes.

This parameter is either a set of integers or a set of object identifiers. However, only object identifiers shall be used within the Systems management context defined in CCITT Rec. X.701 | ISO/IEC 10040. Such object identifiers may be registered outside of this Recommendation | International Standard using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

8.1.2.3 Perceived severity

This parameter defines six severity levels, which provide an indication of how it is perceived that the capability of the managed object has been affected. Those severity levels which represent service affecting conditions ordered from most severe to least severe are Critical, Major, Minor and Warning. The levels defined for use with this mandatory parameter are

- cleared: The Cleared severity level indicates the clearing of one or more previously reported alarms. This alarm clears all alarms for this managed object that have the same Alarm type, Probable cause and Specific problems (if given). Multiple associated notifications may be cleared by using the Correlated notifications parameter (defined below).

  This Recommendation | International Standard does not require that the clearing of previously reported alarms be reported. Therefore, a managing system cannot assume that the absence of an alarm with the Cleared severity level means that the condition that caused the generation of previous alarms is still present. Managed object definers shall state if, and under which conditions, the Cleared severity level is used.
- indeterminate: The Indeterminate severity level indicates that the severity level cannot be determined.
- critical: The Critical severity level indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported, for example, when a managed object becomes totally out of service and its capability must be restored.
- major: The Major severity level indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported, for example, when there is a severe degradation in the capability of the managed object and its full capability must be restored.
- minor: The Minor severity level indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported, for example, when the detected alarm condition is not currently degrading the capacity of the managed object.
- warning: The Warning severity level indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault.

8.1.2.4 Backed-up status

This parameter, when present, specifies whether or not the object emitting the alarm has been backed-up, and services provided to the user have, therefore, not been disrupted. The use of this field in conjunction with the severity field provides information in an independent form to qualify the seriousness of the alarm and the ability of the system as a whole to continue to provide services. If the value of this parameter is true, it indicates that the object emitting the alarm has been backed-up; if false, the object has not been backed-up.

8.1.2.5 Back-up object

This parameter shall be present when the Backed-up status parameter is present and has the value true. This parameter specifies the managed object instance that is providing back-up services for the managed object about which the notification pertains. This parameter is useful, for example, when the back-up object is from a pool of objects any of which may be dynamically allocated to replace a faulty object.

The Back-up object parameter is related to the Back-up object relationship attribute defined in CCITT Rec. X.732 | ISO/IEC 10164-3. The value of this parameter shall be the same as the Back-up object attribute value when the alarm is emitted.

8.1.2.6 Trend indication

This parameter, when present, specifies the current severity trend of the managed object. If present it indicates that there are one or more alarms ("outstanding alarms") which have not been cleared, and pertain to the same managed object as that to which this alarm ("current alarm") pertains. The Trend indication parameter has three possible values

- more severe: The Perceived severity in the current alarm is higher (more severe) than that reported in any of the outstanding alarms;
- no change: The Perceived severity reported in the current alarm is the same as the highest (most severe) of any of the outstanding alarms;
- less severe: There is at least one outstanding alarm of a severity higher (more severe) than that in the current alarm.

In order for Trend indication to be meaningful, the Perceived severity parameter value of each alarm that may be emitted by the managed object must be defined consistently over all of the defined alarm types for that managed object class. Trend indication information is of particular use to managing systems which receive alarm reports from an event forwarding discriminator configured to pass alarms above a Perceived severity level. The severity trend can also be determined by a managing system that monitors the Perceived severity parameter in received alarm reports.

The Trend indication parameter shall not be present if there are no outstanding alarms.

The absence of the Trend indication parameter cannot be taken to indicate the existence or non-existence of outstanding alarms.

8.1.2.7 Threshold information

This parameter shall be present when the alarm is a result of crossing a threshold. It consists of four subparameters

- triggered threshold: The identifier of the threshold attribute that caused the notification;
- threshold level: In the case of a gauge the threshold level specifies a pair of threshold values, the first being the value of the crossed threshold and the second, its corresponding hysteresis; in the case of a counter the threshold level specifies only the threshold value.
- observed value: The value of the gauge or counter which crossed the threshold. This may be different from the threshold value if, for example, the gauge may only take on discrete values.
- arm time: For a gauge threshold, the time at which the threshold was last re-armed, namely the time after the previous threshold crossing at which the hysteresis value of the threshold was exceeded thus again permitting generation of notifications when the threshold is crossed. For a counter threshold, the later of the time at which the threshold offset was last applied, or the time at which the counter was last initialized (for resettable counters).

8.1.2.8 Notification identifier

This parameter, when present, provides an identifier for the notification, which may be carried in the Correlated notifications parameter (see below) of future notifications. Notification identifiers must be chosen to be unique across all notifications of a particular managed object throughout the time that correlation is significant.

A Notification identifier may be reused if there is no requirement that the previous notification using that Notification identifier be correlated with future notifications. Generally, Notification identifiers should be chosen to ensure uniqueness over as long a time as is feasible for the managed system.

8.1.2.9 Correlated notifications

This parameter, when present, contains a set of Notification identifiers and, if necessary, their associated managed object instance names. This set is defined to be the set of all notifications to which this notification is considered to be correlated. The source object instance shall be present if the correlated event report is from a managed object instance other than the one in which the Correlated notifications parameter appears.

The algorithm by which correlation is accomplished is outside the scope of this Recommendation | International Standard.

8.1.2.10 State change definition

This parameter, when present, is used to indicate a state transition, as specified in CCITT Rec. X.731 | ISO/IEC 10164-2, associated with the alarm. In this case, if the managed object class definition includes state change notifications it shall also emit a state change notification as specified in CCITT Rec. X.731 | ISO/IEC 10164-2.

8.1.2.11 Monitored attributes

The Monitored attributes parameter, when present, defines one or more attributes of the managed object and their corresponding values at the time of the alarm. Managed object definers may specify the set of attributes which are of interest, if any. This allows, for example, the timely reporting of changing conditions prevalent at the time of the alarm.

8.1.2.12 Proposed repair actions

This parameter, when present, is used if the cause is known and the system being managed can suggest one or more solutions (such as switch in standby equipment, retry, replace media). This parameter is a set of possibilities specified by the object class definer.

This parameter is either a set of integers or a set of object identifiers. However, only object identifiers shall be used within the Systems management context defined in CCITT Rec. X.701 | ISO/IEC 10040. Such identifiers may be registered using the registration procedures defined for ASN.1 Object Identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

The following note applies to CCITT applications only.

NOTE – Two values with the following semantics have been assigned to this parameter in this Recommendation | International Standard

- no repair action required: This value is used to indicate that the manager is not required to initiate any repair action because it is not the manager's responsibility;
- repair action required: This value is used to indicate that the manager is required to initiate repair action to correct the problem reported in the alarm report. This value also indicates that no specific repair action is proposed by the agent system.

These values may be used if the cause is known and the system being managed can suggest one or more proposed actions to be taken by the recipient of the alarm report.

8.1.2.13 Additional text

This parameter, when present, allows a free form text description to be reported. Understanding the semantics of this field is not required for interpretation of the notification.

This Recommendation | International Standard does not specify the format or meaning of the data contained in the Additional text parameter. The contents are not subject to any test of OSI Management conformance.

8.1.2.14 Additional information

This parameter, when present, allows the inclusion of a set of additional information in the event report. It is a series of data structures each of which contains three items of information: an identifier, a significance indicator, and the problem information.

The identifier subparameter carries a registered object identifier which defines the data type of the information subparameter. The data type must be understood by the managing system in order for the contents of the information subparameter to be parsed. Additional identifiers may be registered using the procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

The significance subparameter is a boolean value which is set to true if the receiving system must be able to parse the contents of the information subparameter for the event report to be fully understood. Even if the Additional information parameter is not fully understood, an event report indication shall be issued to the user. Indication that the Additional information parameter is not fully understood is a local matter.

The information subparameter carries information about the event. This information can be parsed if the identifier is understood.

8.1.3 Event reply

This Recommendation | International Standard does not specify management information to be used in the event reply parameter.

8.2 Managed objects

An Alarm record is a managed object class derived from the Event log record object class defined in CCITT Rec. X.721 | ISO/IEC 10165-2. The Alarm record object class represents information stored in logs as a result of receiving an event report where the event type is one of the alarm types defined in this Recommendation | International Standard.

8.3 Compliance

Managed object class definitions support the functions defined in this Recommendation | International Standard by incorporating the appropriate specification of notifications through reference to the notification templates defined in CCITT Rec. X.721 | ISO/IEC 10165-2. The reference mechanism is defined in CCITT Rec. X.722 | ISO/IEC 10165-4.

A managed object class definition importing one or more of the alarms defined in this Recommendation | International Standard is required, for each use of an alarm, to select the alarm type and probable cause that most closely specifies the real event in the managed object. If the managed object class specifies more than one event for a particular combination of alarm type and probable cause, the Specific problems parameter may be used to uniquely identify the event.

The Additional text parameter may be used to identify and communicate additional or more specific alarm information. However, the preferred method is by registration and use of additional values for the Probable cause and/or Specific problems and/or Additional information parameters.

The Additional information parameter may include diagnostic information and other information relating to the alarm. However, information which can be mapped to the other parameters provided by this Recommendation | International Standard (excepting Additional text) should not be reported using the Additional information parameter.

9 Service definition

9.1 Introduction

This Recommendation | International Standard defines one service which is identified below together with the appropriate parameters.

The alarm reporting service allows one user to notify another user of an alarm detected in a managed object. The originating user has to specify whether or not a reply is required. Further parameters convey the identification of the managed object, the type and time of the alarm, and other relevant management information.

9.2 Alarm reporting service

The alarm reporting service uses the parameters defined in clause 8 of this Recommendation | International Standard in addition to the general M-EVENT-REPORT service parameters defined in CCITT Rec. X.710 | ISO/IEC 9595.

Table 1 lists the parameters for the alarm reporting service.

The Event time, Correlated notifications, and Notification identifier parameters may be assigned by the object emitting the notification or by the managed system. If no Perceived severity is defined for an object class the value shall be assigned by the managed system. The managed system may assign the Trend indication value if the managed object policy allows system assignment of Perceived severity.

10 Functional units

The Alarm reporting function forms a single systems management functional unit.

Table 1 – Alarm reporting parameters

Parameter name	Req/Ind	Rsp/Conf
Invoke identifier	P	P
Mode	P	–
Managed object class	P	P
Managed object instance	P	P
Event type	M	C(=)
Event time	P	–
Event information		
Probable cause	M	–
Specific problems	U	–
Perceived severity	M	–
Backed-up status	U	–
Back-up object	C	–
Trend indication	U	–
Threshold information	C	–
Notification identifier	U	–
Correlated notifications	U	–
State change definition	U	–
Monitored attributes	U	–
Proposed repair actions	U	–
Additional text	U	–
Additional information	U	–
Current time	–	P
Event reply	–	–
Errors	–	P

11 Protocol

11.1 Elements of procedure

11.1.1 Agent role

11.1.1.1 Invocation

The alarm reporting procedures are initiated by the alarm reporting request primitive. On receipt of an alarm reporting request primitive, the SMAPM shall construct an MAPDU and issue a CMIS M-EVENT-REPORT request service primitive with parameters derived from the alarm reporting request primitive. In the non-confirmed mode, the procedure in 11.1.1.2 does not apply.

11.1.1.2 Receipt of response

On receipt of a CMIS M-EVENT-REPORT confirm service primitive containing an MAPDU responding to an alarm reporting notification, the SMAPM shall issue an alarm reporting confirmation primitive to the alarm reporting service user with parameters derived from the CMIS M-EVENT-REPORT confirm service primitive, thus completing the alarm reporting procedure.

NOTE – The SMAPM shall ignore all errors in the received MAPDU. The alarm reporting service user may ignore such errors, or abort the association as a consequence of such errors.

11.1.2 Manager role

11.1.2.1 Receipt of request

On receipt of a CMIS M-EVENT-REPORT indication service primitive containing an MAPDU requesting the alarm reporting service, the SMAPM shall, if the MAPDU is well formed, issue an alarm reporting indication primitive to the alarm reporting service user with parameters derived from the CMIS M-EVENT-REPORT indication service primitive. Otherwise, the SMAPM shall, in the confirmed mode, construct an appropriate MAPDU containing notification of the error, and shall issue a CMIS M-EVENT-REPORT response service primitive with an error parameter present. In the non-confirmed mode, the procedure in 11.1.2.2 does not apply.

11.1.2.2 Response

In the confirmed mode, the SMAPM shall accept an alarm reporting response primitive and shall construct an MAPDU confirming notification and issue a CMIS M-EVENT-REPORT response service primitive with parameters derived from the alarm reporting response primitive.

11.2 Abstract syntax

11.2.1 Managed objects

This Recommendation | International Standard references the following support object for which the abstract syntax is specified in CCITT Rec. X.721 | ISO/IEC 10165-2

– alarmRecord.

11.2.2 Attributes

Table 2 identifies the relationship between the parameters defined in 8.1.2 of this Recommendation | International Standard and the attribute types specifications in CCITT Rec. X.721 | ISO/IEC 10165-2.

Table 2 – Attributes

Parameter	Attribute name
Probable cause	probableCause
Specific problems	specificProblems
Perceived severity	perceivedSeverity
Backed-up status	backedUpStatus
Back-up object	backupObject
Trend indication	trendIndication
Threshold information	thresholdInfo
Notification identifier	notificationIdentifier
Correlated notifications	correlatedNotifications
State change definition	stateChangeDefinition
Monitored attributes	monitoredAttributes
Proposed repair actions	proposedRepairActions
Additional text	additionalText
Additional information	additionalInformation

11.2.3 Attribute groups

There are no attribute groups defined by this Recommendation | International Standard.

11.2.4 Actions

There are no specific actions defined by this Recommendation | International Standard.

11.2.5 Notifications

Table 3 identifies the relationship between the notifications defined in 8.1.1 of this Recommendation | International Standard and the notification type specifications in CCITT Rec. X.721 | ISO/IEC 10165-2.

Table 3 – Notifications

Alarm type	Notification type
Communications alarm	communicationsAlarm
Quality of service alarm	qualityofServiceAlarm
Processing error alarm	processingErrorAlarm
Equipment alarm	equipmentAlarm
Environmental alarm	environmentalAlarm

11.2.6 Probable causes

Table 4 identifies the relationship between the Probable causes defined in 8.1.2.1 of this Recommendation | International Standard and the ASN.1 value references defined in CCITT Rec. X.721 | ISO/IEC 10165-2.

11.2.7 Perceived severity values

Table 5 identifies the relationship between the values defined for the Perceived severity in 8.1.2.3 of this Recommendation | International Standard and the ASN.1 value references defined in CCITT Rec. X.721 | ISO/IEC 10165-2.

Table 5 – Perceived severity values

Perceived severity	ASN.1 value reference
Cleared	cleared
Indeterminate	indeterminate
Critical	critical
Major	major
Minor	minor
Warning	warning

Table 4 – Probable causes

Probable cause name	DMI value reference
Adapter error	adapterError
Application subsystem failure	applicationSubsystemFailure
Bandwidth reduced	bandwidthReduced
Call establishment error	callEstablishmentError
Communications protocol error	communicationsProtocolError
Communications subsystem failure	communicationsSubsystemFailure
Configuration or customization error	configurationOrCustomizationError
Congestion	congestion
Corrupt data	corruptData
CPU cycles limit exceeded	cpuCyclesLimitExceeded
Dataset or modem error	datasetOrModemError
Degraded signal	degradedSignal
DTE-DCE interface error	dTE-DCEInterfaceError
Enclosure door open	enclosureDoorOpen
Equipment malfunction	equipmentMalfunction
Excessive vibration	excessiveVibration
File error	fileError
Fire detected	fireDetected
Flood detected	floodDetected
Framing error	framingError
Heating/ventilation/cooling	heatingOrVentilationOrCoolingSystemProblem
Humidity unacceptable	humidityUnacceptable
I/O device error	inputOutputDeviceError
Input device error	inputDeviceError
LAN error	lANError
Leak detected	leakDetected
Local node transmission error	localNodeTransmissionError
Loss of frame	lossOfFrame
Loss of signal	lossOfSignal
Material supply exhausted	materialSupplyExhausted
Multiplexer problem	multiplexerProblem
Out of memory	outOfMemory
Output device error	outputDeviceError
Performance degraded	performanceDegraded
Power problem	powerProblem
Pressure unacceptable	pressureUnacceptable
Processor problem	processorProblem
Pump failure	pumpFailure
Queue size exceeded	queueSizeExceeded
Receive failure	receiveFailure
Receiver failure	receiverFailure
Remote node transmission error	remoteNodeTransmissionError
Resource at or nearing capacity	resourceAtOrNearingCapacity
Response time excessive	responseTimeExcessive
Retransmission rate excessive	retransmissionRateExcessive
Sofware error	sofwareError
Sofware program abnormally terminated	sofwareProgramAbnormallyTerminated
Sofware program error	softwareProgramError
Storage capacity problem	storageCapacityProblem
Temperature unacceptable	temperatureUnacceptable
Threshold crossed	thresholdCrossed
Timing problem	timingProblem
Toxic leak detected	toxicLeakDetected
Transmit Failure	transmitFailure
Transmitter Failure	transmitterFailure
Underlying resource unavailable	underlyingResourceUnavailable
Version mismatch	versionMismatch

11.3 Negotiation of the alarm reporting functional unit

This Recommendation | International Standard assigns the following object identifier

{joint-iso-ccitt ms(9) function(2) part4(4) functionalUnitPackage(1)}

as a value of the ASN.1 type FunctionalUnitPackageId defined in CCITT Rec. X.701 | ISO/IEC 10040 for negotiating the following functional unit

0 alarm reporting functional unit

where the number identifies the bit position assigned to the functional unit, and the name references the functional unit as defined in clause 10.

Within the Systems management application context, the mechanism for negotiating the alarm reporting functional unit is described by CCITT Rec. X.701 | ISO/IEC 10040.

NOTE – The requirement to negotiate functional units is specified by the application context.

12 Relationships with other functions

Control of the alarm reporting service is provided by mechanisms specified in CCITT Rec. X.734 | ISO/IEC 10164-5. The alarm reporting service may exist independently of the control mechanisms of CCITT REC. X.734 | ISO/IEC 10164-5.

The notifications defined by this function may report instances of the back-up relationship as defined in CCITT Rec. X.732 | ISO/IEC 10164-3.

13 Conformance

There are two conformance classes; general conformance class and dependent conformance class. A system claiming to implement the elements of procedure for the systems management services defined in this Recommendation | International Standard shall comply with the requirements for either the general or the dependent conformance class as defined in the following clauses. The supplier of the implementation shall state the class to which conformance is claimed.

13.1 General conformance class requirements

A system claiming general conformance shall support this function for all managed object classes that import the management information defined in this Recommendation | International Standard.

13.1.1 Static conformance

The system shall

a) act in the role of manager or agent or both with respect to the alarm reporting functional unit;

b) support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 and named {joint-iso-ccitt asn1(1) basic encoding(1)}, for the purpose of generating and interpreting the MAPDUs defined by the abstract data types referenced in 11.2.5 of this Recommendation | International Standard.

13.1.2 Dynamic conformance

The system shall, in the role(s) for which conformance is claimed, support the elements of procedure defined in this Recommendation | International Standard for the alarm reporting service.