SIF-016-1997

(SIF Document #SIF-NM-9606-050R1)

SIF APPROVED DOCUMENT

PROJECT: Distributed Network Management Environment

SUBJECT: Requirements for SIF OS Platforms

SOURCE: Distributed Network Management Environment (DNME) Subgroup

CONTACT: Connie Hunt (editor and DNME chair)
Southwestern Bell
One Bell Center
Room 34-D-8
St. Louis, MO 63101
314-235-0260
ch9578@momail.sbc.com

DATE: December 10, 1997

ABSTRACT: This document defines communications and management services requirements for a SIF Operations Systems Platform that are primarily for a CMISE environment.. A SIF OS Platform is defined as a set of components (e.g. communications stacks, tools, management services, security services, etc.) that can be purchased from a single supplier or integrated from multiple suppliers, and can be used as a uniform environment for the execution of SONET applications.

This document has received the approval of the SONET Interoperability Forum (SIF).

December 11, 1997

Table of Contents

This document has received the approval of the SONET Interoperability Forum (SIF).

December 11, 1997

1 Introduction

1.1 Purpose

The charter of the SIF Distributed Network Management Environment (DNME) subgroup is to define required Operations Systems (OS) Platform services that can be offered to SONET applications in a TMN environment that speed application development and enable application integration in a multi-supplier environment. The subgroup will also define required OS Platform services that contribute to the manageability of the environment, which may have varying degrees of distribution.

A SIF OS Platform is defined as a set of components (e.g. communications stacks, tools, management services, security services, etc.) that can be purchased from a single supplier or integrated from multiple suppliers, and can be used as a uniform environment for the execution of SONET applications.

Following are objectives of the DNME work:

- Define requirements to support interoperability, integration of multi-vendor applications, application portability, etc.
- Leverage existing and emerging standards and computing technologies.
- Identify what might be lacking for a SIF environment and propose solutions
- Allow for manageable application distribution, scalability and reliability.

Service Provider responses to a SIF network management survey that was completed in early 1997, indicated that there was a high priority for defining a common OS platform for multiple supplier applications. The majority of Service Provider members indicated that they prefer a UNIX operating system for the SONET environment, but Windows/NT was also of interest. There was also high interest in developing guidelines for hardware and software reliability, and addressing scalability and management issues.

This document defines SIF OS Platform requirements for communications and management services. These services are primarily for a CMISE environment. Future work will address other issues of importance to Service Providers.

In this document statements of requirements and objectives are highlighted in ***bold italics*** text.

1.2 Scope

OS Platform requirements to support application implementations of TMN layers EML, NML, and SML within a TMN are within the scope of this specification. Requirements for network elements and craft interface terminals are specified in other SIF documents.

Future work on Application Programming Interfaces (API), such as the NMF TMN/C++ APIs, will be done under the SIF OS/CIT Software Platform Architecture.

2 Communications Requirements

2.1 Management Communications

In February 1996, SIF approved SIF-129-1295R1, *CMISE Base Network Management Platform Requirements*. Sections 2.1, 2.3 and 3.1 incorporate SIF-129-129R1 and make it obsolete.

When CMISE is required, the SIF OS Platform shall support the CMIP communications requirements in Q.812-1996 [1], which specifies -

- ISP 11183-1: 1992, Specification of ACSE, Presentation and Session Protocols for use by ROSE and CMISE, and
- ISP 11183-2: 1992, AOM12 - Enhanced Management Communications.

For OS to NE CMISE communications, the Platform shall support the SIF CMISE Profile, SIF-TA-9601-006-R2, which is more specific (less options) than the above ISPs.

2.2 File Transfer

For platforms that support file transfer for SONET NE software download, and memory backup and restore, the SIF OS Platform shall support the SIF FTAM profile in accordance with SIF-95-002R2.

2.3 Communications Stacks

For CMISE communications, a SIF OS Platform shall support the following profiles for TP4/CLNP over LAN and over X.25. The Platform shall also support CMISE over RFC1006 [2] ***with TCP/IP*** [3]***.***

---

[1] AOM12 was supplemented by Q.812-1996 as follows: "Applications may override the APDU size of 10K specified in AOM12 if a larger size is needed."

[2] RFC1006 is being revised by IETF. The draft RFC is called "ISO Transport Service on top of TCP (ITOT)". The goal is to provide enhancements without introducing interoperability issues with existing RFC1006 implementations.

[3] TCP/IP is not supported on the SONET DCC. Interworking of CLNP and IP is an open issue which the SIF Architecture subgroup is investigating.

- ***ITU-T Q.811 CLNS1 (LAN) Protocol Profiles,*** which specifies -
  ISP 10608-1 and ISP 10608-2:1992, Connection-mode Transport Service over Connectionless-mode Network Service - Part 2: TA51 Profile including Subnetwork-dependent Requirements for CSMA/CD LANs. (TP4/CLNS over CSMA/CD LAN)

- ***ITU-T Q.811 CLNS2 (X.25) Protocol Profiles***, which specifies -
  ISP 10608-1 and ISP 10608-5:1992, Connection-mode Transport Service over Connectionless-mode Network Service - Part 5: TA1111/TA1121 Profile including Subnetwork-dependent Requirements for X.25 Packet Switched Data Networks using Virtual Calls. (TP4/CLNS over X.25)

- ***ITU-T Q.811 RFC1006 with TCP/IP***

Communicating applications should agree on which stack will be used for an interface, so that mediation functions within the DCN are minimized.

For NE-to-OS FTAM communications, the SIF OS Platform shall support the above TP4/CLNS over CSMA/CD LAN specification.

The SIF OS Platform shall support a 10Base-T LAN connection.

3 Management Functions and Services

3.1 System Management Functions

System Management Functions are application functions common to all TMN (CMISE) applications (e.g. state management, alarm reporting), or might be used by a specific type of TMN application (e.g. performance applications). There is an increasing number of management functions being standardized by ITU-T and ISO. Appendix A lists the management functions currently of interest. It provides a description of the functions by standard and identifies any associated Management Function Profiles (i.e., AOM2xx).

A SIF OS Platform shall support the following Management Function Profiles and standards (previously identified in SIF-129-1295R1):~~.~~

NMF TMN Basic Management Platform Component Set, which specifies -

- ISP 12060-1:1994, AOM211 - General Management Capabilities,
- ISP 12060-4: 1994, AOM221, General Event Report Management,
- ISP 12060-5: 1994, AOM231 - General Log Control,

- NMF 021, Managed Object Naming, Issue 2, 10/95, and
- NMF 015, Shared Management Knowledge, Issue 1, 10/92 + Errata, Issue 1, 10/95, or draft X.750/DIS 10164-16, Management Knowledge Management Function.

The following additional Management Function Profiles have been standardized. The associated Management Functions are described in Appendix A.

AOM242 - Security Management Capabilities
(Security Alarm Reporting Function and Security Audit Trail Function)

AOM243 - General Security Services and Mechanisms for Management
AOM2432 - Access Control
AOM24321 - General Access Control
AOM24322 - Access Control Lists with Item Rules
AOM24223 - Access Control Lists with Global Rules
AOM24224 - Security Label
AOM24225 - Security Label with additional constraints
AOM24226 - Capability List

AOM252 - Metric Objects

AOM253 - Summarization Objects

It is an objective for the SIF OS Platform to support these profiles, as well as those for Scheduling and Software Management Functions.

3.2 Security

T1.243, *Baseline Security Requirements for the Telecommunications Management Network (TMN)*, specifies the minimum security features that are required of a TMN. Many of these features are applicable to the SIF OS Platform. Depending on a specific application's security risk assessment, security features that are not supported by the OS Platform will need to be provided by the application.

The SIF OS Platform shall support applicable T1.243 security features.

T1.233, *Security Framework for Telecommunications Management Network (TMN) Interface*, describes the following OSI security services for meeting TMN security requirements:

- Authentication
- Access Control

- Data Integrity
- Data Confidentiality
- Non-repudiation

Again, depending on an application's security risk, varying degrees of these security services will be required. Electronic Bonding applications (e.g., those having TMN X interfaces), some of which require all of these security services, depend primarily on the applications to provide them. SIF is currently addressing internal SONET management (e.g., within a single TMN), where the TMN X interface is not an immediate issue for security. However, as the NE operations interface becomes more open (e.g., OSI networking over Ethernet) the need for enhanced NE-to-OS security is being considered. In anticipation of this, SIF has identified OSI Entity Authentication and Access Control as the security services with the highest priority for support by the SIF OS Platform.

3.2.1 Entity Authentication

The SIF OS Platform shall support strong entity authentication, utilizing asymmetric encryption (Public-Key Crypto Systems (PKCS)). The mechanism for exchanging authenticating information is by making use of the ACSE Authentication Functional Unit as described in T1M1.5/97-114-Rx, **Security for TMN Management over the TMN Q3 Interface** ***[T1.Q3sec].***

The following public key encryption algorithm shall be supported as a default:

- ***public key encryption - RSA PKCS: user key shall be 700 bits or larger; Certification Authority key shall be 1024 bits or larger***

Negotiation of encryption algorithms and related keys at association establishment time is optional.

When public key encryption is used, a Certification Authority and an X.500 directory service shall be used for X.509 public key certificates as specified in T1.252, **Security for the Telecommunications Management Network (TMN) Directory.** ***The SIF OS Platform shall support a Directory User Agent (DUA) capability for retrieving public key certificates and for certificate revocation lists.***

The SIF OS Platform shall support strong authentication of users by use of X.509 certificates. A User Authentication mechanism may optionally utilize security tokens (smart card, secured floppy disk, etc.) to authenticate users.

3.2.2 Access Control

Access control capabilities generally rely on proper identification and authentication of users and communicating entities. For OSI interfaces, three areas where access control mechanisms are needed are for association establishment, management operations and event notifications.

For CMISE communications, the SIF OS Platform shall support an access control mechanism that is consistent with [T1.Q3sec].

It is an objective that the SIF OS Platform support both access control list (ACL) and access control certificate (ACC) mechanisms. For ACC, X.509 version 3 extensions shall be used as specified in [T1.Q3sec]. Further work is needed to determine if SONET NEs should support ACL or ACC.

It is an objective that the SIF OS Platform support ITU-T X.741 for management of all local access control information, including lists of target objects in the access classes and access control lists (ACL). A subset of X.741 is to be defined and profiled in future work.

At a minimum, ***the SIF OS Platform shall support the following levels of access control (access classes):***

- ***data monitoring operations***
- ***non-service affecting operations***
- ***service affecting operations***
- ***administrative operations***

3.2.3 Data Security

Depending on the sensitive nature of the data being communicated, various levels of data security may be required. There are two types of data security services: data integrity and data confidentiality. T1M1.5/97-114-Rx, *Security for TMN Management over the TMN Q3 Interface* [T1.Q3sec], describes methods for data origin authentication, whole PDU protection for data confidentiality, integrity and non-repudiation.

When data security is required, the SIF OS Platform shall support the mechanisms and default algorithms specified in [T1.Q3sec].

3.2.4 Security for Application Protocols

The following sections on CMISE, FTAM and TL1 intend to summarize the security options available for these application layer protocols.

3.2.4.1 CMISE Security

It is intended that CMISE communications be authenticated at association set up time using the ACSE Authentication Functional Unit. For associations that are long running (e.g. for alarm monitoring), it is recommended that keys be re-established periodically by using a mechanism supported by STASE-ROSE as described in T1.259.

Depending on the sensitive nature of the data being communicated, data security may be required. Mechanisms supported by STASE-ROSE may be used for data security as described in T1.259.

3.2.4.2 FTAM Security

It is intended that FTAM communications be authenticated at association set up time using the ACSE Authentication Functional Unit. Information about keys and other security parameters will be conveyed in ACSE messages as described in T1.259.

Depending on the sensitive nature of the data being communicated, data security may be required. Exchanging information on data security methods and parameters is best done in separate communications or manual processes.

3.2.4.3 TL1 Security

SONET NE to OS security requirements are defined in GR-253, section 6.1.6 on System Administration and Security. Although TL1 over OSI is not a TMN interface, SIF could take advantage of OSI security services to enhance existing TL1 security by using the ACSE Authentication Functional Unit for authenticating entities at association set up time as described in T1.259. For associations that are long running (e.g., for alarm monitoring), the associations may be restarted periodically.

3.2.5 Certificate Management

T1.252 describes how the Directory is populated with security information. A schema for storage of certificates is to be defined.

It is an objective that, when an X.500 Directory System is used for storage of certificates, the SIF OS Platform shall have the ability to retrieve the certificate of the target entity (e.g., agent system, SONET NE) from the Directory. It is also an objective that the SIF OS Platform and the X.500 Directory System support use of Certificate Revocation Lists.

3.2.6 Security Reporting

It is an objective that the SIF OS Platform shall support the Security Alarm Reporting Functional Unit defined in X.736 and the Security Audit Trail Reporting Functional Unit defined in X.740 as specified in T1.233.

AOM242 profile is to be reviewed for use in a security reporting service.

3.3 Directory Services

An X.500 Directory System is needed in a SONET environment for centralized management of information that is used for name to address resolution, security, and other services.

A SIF OS Platform shall support an X.500 Directory User Agent (DUA) and Directory Access Protocol (DAP) as specified in ANSI T1.245. These are required at a minimum for security (strong authentication with public key).

For a SIF OS Platform that hosts an X.500 Directory, the Platform shall support X.500 Directory System Agent (DSA) and the Directory schema as specified in T1.245.

For a SIF OS Platform that hosts an OSI level 1 routing area Registration Manager, the Platform shall support the Registration Manager (RM) and the Registration Request Protocol (RRP) as specified in T1.245.

A SIF OS Platform may also host a Registration Agent so that it can learn the address of the X.500 Directory and optionally register information about its own local directory. ***For a SIF OS Platform that hosts a Registration Agent, the Platform shall support the Registration Agent (RA) and the Registration Request Protocol (RRP) as specified in T1.245.***

4 User Interface

SIF has approved SIF-NM-9602-018R2, *Design Principles for the Development of OAM Graphical User Interfaces,* as the SIF guide for "common look and feel".

A SIF OS Platform that provides a graphical user interface for hosted applications shall support the design principles in SIF-NM-9602-018R2.

Future work may be needed to define requirements for application integration at the user interface.

Acronyms

ACC	Access Control Certificate
ACI	Access Control Information
ACL	Access Control List
ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation 1
CLNP	Connectionless-mode Network Protocol
CLNS	Connectionless-mode Network Service
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DAP	Directory Access Protocol
DCN	Data Communication Network
DSA	Directory System Agent
DUA	Directory User Agent
EFD	Event Forwarding Discriminator
EML	Element Management Layer
FTAM	File Transfer Administration and Management
GDMO	Guidelines for the Definition of Managed Objects
ISP	International Standardized Profile
LAN	Local Area Network
MO	Managed Object
NE	Network Element
NMF	Network Management Forum
NML	Network Management Layer
OAM	Operations, Administration and Maintenance
OS	Operations System
OSI	Open Systems Interconnection
PKCS	Public Key Crypto System
RA	Registration Agent

This document has received the approval of the SONET Interoperability Forum (SIF).

December 11, 1997

RM	Registration Manager
ROSE	Remote Operations Service Element
RRP	Registration Request Protocol
RSA	Rivest Shamir Adelman
SML	Service Management Layer
STASE-ROSE	Security Transformations Application Service Element - ROSE
TL1	Transaction Language 1
TMN	Telecommunications Management Network
TP4	Transport Protocol class 4

References

SIF-129-1295R1: *CMISE Base Network Management Platform Requirements*

SIF-NM-9602-018R2: *Design Principles for the Development of OAM Graphical User Interfaces*

SIF-TA-9601-006-R2: *SIF CMISE Profile*

SIF-95-002R2: *SIF FTAM profile*

SIF-DN-9706-045Rx: *SIF OS/CIT Software Platform Architecture Specification*

SIF-RL-9611-088R2*: NE-NE Remote Login Implementation Requirements Specification*

SIF-116-0895-R3: *Remote Login Implementation Requirements Specification*

GR-253-CORE, *SONET Transport Systems: Common Generic Criteria*, Issue 2, December, 1995

GR-1469-CORE, *Generic Requirements on Security for OSI-Based Telecommunications Network Interfaces*, Issue 1, September, 1994

T1.233, *Security Framework for Telecommunications Management Network (TMN) Interface*, 1993

T1.243, *Baseline Security Requirements for the Telecommunications Management Network (TMN)*, 1995

T1.245, *Directory Service for Telecommunications Management Network (TMN) and Synchronous Optical Network (SONET)*, 1995

T1.252, *Security for the Telecommunications Management Network (TMN) Directory, 1996*

T1.259, *Security Transformations Application Service Element for ROSE*, 1997

[T1.Q3sec] T1M1.5/97-114-Rx, *Security for TMN Management over the TMN Q3 Interface*, August 1997

ITU-T X.741, *Systems Management: Objects and Attributes for Access Control*

This document has received the approval of the SONET Interoperability Forum (SIF).

December 11, 1997

ITU-T Q.811: *Lower Layer Protocol Profiles for the Q3 and X Interface*, 1996 Revision

ITU-T Q.812: *Upper Layer Protocol Profiles for the Q3 and X Interface*, 1996 Revision

NMF CS302: *TMN Basic Management Platform Component Set*, Issue 1.0, October 1995:

NMF TR115, *An OMNIpoint TMN Design Guide: Using ISPs to Implement the Management Communications Aspects of Q3 and X Interfaces*, Issue 1.0, October 1995

NMF 021, *Managed Object Naming*, Issue 2.0, October 1995

NMF 015, *Shared Management Knowledge*, Issue 1.0, October 1992 + Errata, Issue 1.0, October 1995

ISO IEC CD 10164-16.2: *Information Technology - Open Systems Interconnection - Systems Management: Management Knowledge Management Function*, June 20, 1994

Appendix A: System Management Functions

This section provides a summary of the system management functions defined in the ITU recommendations and ISO/IEC standards that are of interest to this project.

Most of the system management functions refer to GDMO/ASN.1 definitions of X.721 | 10165-2.

Profiles mentioned in this table are:

AOM211, General Management Capability
AOM221, General Event Report Management
AOM231, General Log Control
AOM242, Security Management Capabilities
AOM252, Metric Objects
AOM253, Summarization Objects

Standards (ITU/ ISO/IEC) and Profiles	Short Title	Description/Summary
X.730 | 10164-1 Referenced by: AOM211 AOM221 AOM231	Object Management Function	Motivation and Requirements: TMN applications should be designed and built based on the principles of the TMN architecture. The standards groups have defined a number of features in the form of objects, packages, notifications and attributes whose goal is to provide a generic configurable framework around which other objects may be commonly managed. Applications that leverage off this work realize the benefits of object-oriented design and programming techniques and practices. Model: Each resource that is subject to systems management is represented by a managed object. Managed objects can be created and deleted, and values of attributes of managed objects can be changed. Object management describes services for the reporting of creation and deletion of managed objects • the reporting of changes to attribute values of managed objects

		• Object management describes pass-through services.
X.731 | 10164-2 Referenced by: AOM211 AOM221 AOM231	State Management Function	Motivation and Requirements: Every managed object can have state information attached to it like whether the resource is physically installed and working (operational), whether or not the resource is actively in use at a specific instant (usage) or permission to use or prohibition against using the resource (administrative) for example. State management describes a service for the reporting of state changes of managed objects. It provides generic definitions for querying and changing the management state of an object instance. The MIS-user needs the ability to examine and be notified of changes in state, to monitor overall operability and usage of resources in a consistent manner, and to control the general availability of specific resources. Model: The state management provides for • the reporting of changes in the state attributes; • reading the state attributes; • changing the state attributes. Generic states representing the status of a managed resource are: • operational state • usage state • administrative state
X.732 | 10164-3 Referenced by: AOM211	Attributes for Representing Relationships	Motivation and Requirements: The ability to implement object-oriented systems that utilize functions like inheritance and containment allow for the implementation of flexible and extensible management applications. Another very powerful mechanism that facilitates a flexible solution is the ability to relate un-contained objects. A mechanism that allows both users and application developers configure and manage relationships between objects enables rapid behavioral changes to be applied to the operation of the management system.

		The management user needs the ability to examine the relationship among various parts of the system or systems, to see how the operation of one part of the system depends upon or is depended upon by other parts. Model: A relationship is defined by a set of rules that describe how the operation of one part of an open system affects the operation of other parts. Categories of relationships • reciprocal relationship • one-way relationship Types of relationships (roles) • service relationship (provider and user object) • peer relationship (peer) • fallback relationship (primary, secondary) • back-up relationship (back-up and backed-up object) • group relationship (owner, member) Generic definitions of this recommendation: • generic attributes • generic notifications • managed objects
X.733 | 10164-4 Referenced by: AOM211 AOM231	Alarm Reporting Function	Motivation and Requirements: As the network grows to incorporate new equipment types and technologies, so too does the number of alarm messages. Having the ability to generically handle alarms messages in a consolidated manner allows management applications to easier incorporate these new messages. Reporting of alarms, errors and related information, in a standard fashion. Model: This recommendation defines: • event types (communications alarm, quality of service alarm, processing error alarm, equipment alarm, environmental alarm)

		• event information (probable cause, specific problems, perceived severity, backed-up status, back-up object, trend indication, threshold information, notification identifier, correlated notifications, ...)
X.734 | 10164-5 Referenced by: AOM221	Event Report Management Function	Motivation and Requirements: The requirements to be satisfied are: • the definition of a flexible event report control service which allow systems to select which event reports are to be sent to particular management systems. • the specification of the destination to which event reports are to be sent. • the specification of a mechanism to control the forwarding of event reports • the ability for an external managing system to modify the conditions used in the reporting of events • the ability to designate a backup location to which the event reports can be sent if the primary location is not available. Model : The model describes the conceptual components that provide for remote event reporting and local processing of potential event reports. The model is based on discriminator, EFD objects which allow to control event report generation by specifying filters, destinations and scheduling information. It also describes the relationship to the log control function.
X.735 | 10164-6 Referenced by: AOM231	Log Control Function	Motivation and Requirements: For the purpose of many management functions it is necessary to be able to preserve information about events that may have occurred or operations that may have been performed by or on various objects. In OSI management these resources are modeled by logs and log records contained in the logs. The above needs give rise to the following requirements: • the definition of a flexible log control service which allow selection of records that are to be logged by a management system in a particular log • the ability for an external system to modify the criteria used in logging records

		• the ability for an external system to determine whether the logging characteristics were modified or whether log records have been lost • specification of a mechanism to control the time during which logging occurs • the ability for an external system to retrieve and delete log records • the ability for an external system to create and delete logs Model: • logs store incoming event reports and local system notifications • logging is controlled through filters, scheduling information, log size, "log full" action
X.736 | 10164-7 Referenced by: AOM242	Security Alarm Reporting Function	Motivation and Requirements: The security management user needs to be alerted whenever an event indicating an attack or potential attack on system security has been detected. Model: • X.721 defines 5 security alarm types (integrity violation, operational violation, physical violation, security service or mechanism violation, time domain violation). • Security attacks may be detected by a security service/mechanism/process. This service/mechanism/process triggers one of the security alarm types. • security alarms may be logged according to X.735 (see securityAlarmReportRecord) • control of the security alarm reporting service is provided by mechanisms specified in X.734, but may exist independently
X.738 | 10164-13 Referenced by: AOM253	Summarization Function	Motivation and Requirements: Summarization provides the ability to aggregate observed attribute values and/or provide ensemble statistical information about observed attribute values. The summarization function shall provide for: • the ability for a managing system to request

		summarization of attribute values • the ability to summarize values • the ability to provide summarized information gathered • the scheduling of summarization activity over a specified period of time • the aggregation of observed attribute values on a single managed system • the identification of the managed objects and their attributes to be summarized • a mechanism for the selection of managed objects which have the same set of attributes to be summarized • the ability to specify the selection criteria for managed objects to be observed and their attributes to be summarized, at any point in time • the ability to provide ensemble statistics of the information gathered • the ability for a managed system to send event reports to a managing system • the concise reporting of large quantities of summarized information Model: • defines a set of summarization objects (scanners) which scan attributes of a well-defined set of "objects under observation". The summarization functions retrieves observed attribute values and forwards it to the manager as event reports or as a summary report result if the manager requested the summary report through a summary request action. • all scanner objects are subclasses of the Scanner object defined in X.739
X.739 | 10164-11 Referenced by: AOM252	Metric Objects and Attributes	Motivation and Requirements: In terms of functionality, the requirements to be satisfied are: • the definition of statistical tools to derive metrics to characterize performance • the definition of a monitoring function which provides metrics which can be used to determine the resource request rate, resource rejection rate, and resource utilization • the specification of mechanisms to obtain these metrics • the specification of notification to be

		generated when these metrics exceed threshold values, and the ability to include additional performance information into those notifications • the specification of mechanisms to control the operation of this function • the ability of an external managing system to modify parameters defined and used in this monitoring function • the ability to model either physical capacity limitations or those limitations imposed by administrative decisions • the scheduling of metric monitoring over a specified interval of time • the ability for a managing system to enable and disable performance measurements independent of the managed objects under observations Model: • Provides managers of performance with tools to observe characteristics of resources either directly within observable managed objects or through the use of metric objects. The tools include methods to observe resources and to provide statistics. These tools also include thresholds to generate notifications. • the metric object model defines 4 steps (data capture, data conversion, data enhancement, data analysis). Those steps depend on algorithms defined in metric objects. • defines a severity indicating gauge-threshold model • defines a model for workload monitoring
X.740 | 10164-8 Referenced by: AOM242	Security Audit Trail Function	Motivation and Requirements: The security management user requires the ability to record a security audit log, security-related events that occur in the management domain. The types of security-related event that may be subject to auditing include, but are not limited to • connections, • disconnections, • security mechanism utilization, • management operations, and • usage accounting. Model:

		Security-related event are logged according to X.735, i.e. the security audit trail log is a log as defined in X.735. This standard defines a securityAuditTrailRecord MO and two independent notifications (serviceReport, usageReport) and corresponding GDMO/ASN.1 definitions.

X.741 | 1016-9 Referenced by: AOM242	Objects and Attributes for Access Control	Motivation and Requirements: Control of access to management information is required in each of the following cases; • to protect management information from unauthorized creation, deletion, modification or disclosure by means of OSI management operations • to ensure that initiators are only able to use the management operations for which access rights were granted during application association establishment; and • to prevent management information from being transmitted to unauthorized recipients by means of confirmed or non-confirmed event reports Model: • access control for OSI management is based on the model for access control defined in X.812, i.e. based on ACL schemes, capability schemes, context based schemes and label based schemes. • a security domain is defined by an access control policy and a group of elements (MOs, attributes, etc.). Within a security domain a single access control policy is enforced. • an access policy incorporates one or more sets of rules. • access control of event reports is effected by applying access control to management operations upon event forwarding discriminators. • the access control decision function requires access control information (ACI) for use in the decision making process. This process depends on access control procedures and access control rules. • ACI includes access control rules, the identity of the initiator, the management information identities to which access has been requested, etc.
X.742 |10164-10	Usage Metering Function for Accounting Purposes	Motivation and Requirements: The usage metering function should fulfill the requirements by which resource utilization is determined so that the data that are gathered may be used for the process of accounting management and

		the generation of bills. Model: Accounting for resource utilization has three sub-processes. These sub-processes are: • the usage metering process - This process is responsible for the creation of usage metering records as a consequence of the occurrence of accountable events in systems. The usage metering process is also responsible for logging of the usage metering records. Several accountable events may result in a single usage metering record. In general use of a service which demands the use of several resources will give rise to several usage metering records. • The charging process - This process is responsible for collecting the usage metering records which pertain to a particular service transaction in order to combine them into service transaction records. In addition, pricing information (according to a tariff-system) is added to the service transaction records. The charging process is also responsible for logging the service transaction records. • The billing process - This process is responsible for collecting the service transaction records and selecting from these the ones which pertain to a particular service subscriber over a particular time-period and produce the bill from these. • defines algorithms and GDMO/ASN.1 definitions (3 MOs) for this purpose.
X.744 | 10164-18	Software Management Function	Motivation and Requirements: Software Management is one of the services that may be provided in a distributed operations environment. It includes management of a system for delivery of software and the management of software within a system. It includes the following operations: • Backup and Restore - applied to software items • Create and Delete - applied to software items • Deliver - applied to a coordinated set of software items • Execute Program - applied to executable software • Install - to customize software for use

		• Revert - to cause an installed Software Unit managed object to revert back to not being installed • Set Administrative State - can be used to make installed software available or unavailable for use • Validate - to check the integrity of software Model: • Defines four object classes: software, software unit, executable software, and software distribution. • Actions defined are: backup, deliver, execute program, install, restore, revert, terminateValidation, and validate. • Three notifications are defined: autoBackupReport, autoRestoreReport, and deliverResultNotification.
X.745 | 10164-12	Test Management Function	Motivation and Requirements: While the need for functionally rich, easy to use enabling technologies is key for accelerating the deployment of TMN applications so too are the test tools used during the development, simulation, troubleshooting and maintenance phases. The ability to simulate the responding interacting application is key, whether it be an agent or manager, while the specific solution is under development, analysis, design or maintenance. Superior test tools allows for focus on application design and development thereby reducing the time to market with solutions. Model: The execution of a test involves two or more application processes. The simplest test involves just two, a managing process that initiates the test, the test conductor, and an agent process that executes the test, the test performer. The test performer is requested to perform the test by the test conductor. A test request is directed to a managed object, being managed by the test performer, which has functionality to receive and respond to such requests. Such functionality is called the test action request receiver (TARR) functionality. Managed objects which refer to functionalites that are the subjects of

		test, MORT, are identified in test requests. Each test shall involve one or more MORT. For any test, the TARR may be part of the functionality of either a MORT or another managed object. For example, the TAR functionality may be part of a managed object which exists expressly for the purpose of receiving test requests.

X.746 | 10164-15	Scheduling Function	Motivation and Requirements: In terms of functionality, the requirements to be satisfied are: • provide a function that can schedule a number of activities within multiple managed objects according to a single schedule. • be able to specify the time duration that the schedule is active. • for schedules that control the interval of operation of an activity within a managed object, the start and stop time should be defined as the actual time within a 24-hour clock. • provide a function that can schedule aperiodic and periodic triggering of an activity. Model: Scheduling can be modeled as a part of the managed object whose operation or activity is to be scheduled, or as a separate managed object. Characteristics for the control of a schedule can be imported into a managed object class or can be defined as a separate managed object. These two ways of defining scheduling of a managed object are termed internal and external scheduling, respectively. The activities which can be controlled by scheduling are defined as part of the scheduled managed object (SMO) class.