Functional Requirements for Network Management

Use Case Description[1]

1. Descriptions of Function

All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work should be so noted.

1.1 *Function Name*

Name of Function
Enterprise Management (EM) Function.

1.2 *Function ID*

IECSA identification number of the function

1.3 *Brief Description*

Describe briefly the scope, objectives, and rationale of the Function.

Objective: Enterprise management is the task of ensuring that the networks and systems provide the required services with the specified quality of service to the users and other systems. Most enterprise management architectures use agent-manager relationship where the agents, residing on managed network/system elements, provide network/system management information such as alerts or performance measurements to the manager. The manager reacts to these messages by executing one or more actions such as operator notification, event logging, system shutdown, and automatic attempts at system repair. Management entities also poll end stations, automatically or upon user request, to check the values of certain variables. Agents have information about the managed devices in which they reside and provide that information (proactively or reactively) to management entities within one or more enterprise management systems (EMSs) via a network management protocol. The term enterprise management refers to the combined task of network and system management.

Scope: The functions of an enterprise manager facilitated by an EnergyManagementSystem includes:

- Performance Management which involves measurements of various metrics for network/system performance, analyzing the measurements to determine normal levels, and determination of appropriate threshold values to ensure required level of performance for each service. Examples of performance metrics include network/system throughput, user response times, and line utilization. Management entities continually monitor values of the performance metrics. An alert is generated and sent to the enterprise management system when a threshold is exceeded

[1] Background information includes prior UCI work

- Configuration Management which involves maintaining an inventory of the network and system configuration information. This information is used to assure inter-operability and problem detection. Examples of configuration information include device/system OS name and version, types and capacity of interfaces, types and version of the protocol stacks, type and version of network/system management SW, etc.
- Accounting Management which keeps track of usage per account, billing, and ensures resources are available according to the account requirements.
- Fault Management detects, fixes, logs, and reports network/system problems. Fault management involves determining symptoms through measurements and monitoring, and isolating the problem.
- Security Management which controls access to network/system resources according to security guidelines. Security manager partitions network/system resources into authorized and unauthorized areas. Users are provided access rights to one or more areas. Security managers identify sensitive network/system resources (including systems, files, and other entities) and determine accessibility of users and the resources. Security manager monitors access points to sensitive network/system resources and log inappropriate access.

Typically, network management refers to management of network/system resources such as routers, switches, hubs, customer premises equipment and communication links. We extend the domain of enterprise management to enterprise management, defined as the set of functions needed to manage the following resources:

1. Network resources, as defined above,

2. Systems – Computing resources such as substation automation systems, data concentrators, servers such as Market Interface Servers, applications such as data acquisition and control systems, and database management systems,

3. Service and business functions such as RTP customer pricing service, security and operational policy servers,

4. Power system devices such as IEDs and RTUs,

5. Customer premises equipment such as digital meters and consumer portals, and

6. Storage area networks.

Rationale: Proper execution of enterprise management functions not only supports the power system functional requirements such as ensuring connectivity and enforcement of policies, but also the non-functional requirements such as providing quality of service, ensuring reliable and securing communications.

Status: Enterprise management functions are being carried out within the power system industry. The emphasis of the IECSA is in proper and complete execution of all the relevant functions in addition to proposing a unified management platform to simplify cross-management functions.

1.4 *Narrative*

A complete narrative of the Function from a Domain Expert's point of view, describing what occurs when, why, how, and under what conditions. This will be a separate document, but will act as the basis for identifying the Steps in Section 2.

1.5 *Actor (Stakeholder) Roles*

Describe all the people (their job), systems, databases, organizations, and devices involved in or affected by the Function (e.g. operators, system administrators, technicians, end users, service personnel, executives, SCADA system, real-time database, RTO, RTU, IED, power system). Typically, these actors are logically grouped by organization or functional boundaries or just for collaboration purpose of this use case. We need to identify these groupings and their relevant roles and understand the constituency. The same actor could play different roles in different Functions, but only one role in one Function. If the same actor (e.g. the same person) does play multiple roles in one Function, list these different actor-roles as separate rows.

Grouping (Community)		*Group Description*
Enterprise Management		
Actor Name	*Actor Type (person, device, system etc.)*	*Actor Description*
EnterpriseManager	Person	Person performing the function of enterprise management
EnergyManagementSystem	System	Enterprise Management System – EnergyManagementSystem manager, EnergyManagementSystem agent
Customer	Person	The person/company/user of the network/system services
ServiceProvider	Person	The person/company providing network/system services.
ManagedDevice	device	The entity being managed
ManagedDevice2	device	The entity being managed

Replicate this table for each logic group.

1.6 *Information exchanged*

Describe any information exchanged in this template.

Information Object Name	*Information Object Description*
PerformanceData	Types of performance metrics collected by the NMS
ConfigurationData	Configuration Data sent from Manager to Agent
FaultData	Fault data received sent from Agent to Manager
GetRequest	A request to receive data sent from Manager to the Agent.

1.7 *Activities/Services*

Describe or list the activities and services involved in this Function (in the context of this Function). An activity or service can be provided by a computer system, a set of applications, or manual procedures. These activities/services should be described at an appropriate level, with the understanding that sub-activities and services should be described if they are important for operational issues, automation needs, and implementation reasons. Other sub-activities/services could be left for later analysis.

Activity/Service Name	*Activities/Services Provided*
Object management - Defining resources and attributes	EnergyManagementSystem needs to be aware of resources: routers, hubs, computers, and their attributes.
Defining, modifying and examining relationships	EnergyManagementSystem needs to be aware of the object relationships.
Setting, modifying and examining attribute values	Object attributes need to have values. E.g, number & types of ports per card.
Inventory Management	IM is the task of maintaining types and configuration of resources. The inventory information is required for SW and HW maintenance, determination of faults and recovery, and capacity planning.
Network Discovery	Dynamically creates a representation of the network topology, and configuration of the devices. The data could be collected manually, which is very tedious and often not accurate for a large network, or though an EnergyManagementSystem. Instances of the managed devices and their internal components are created and connections are made. Components and info on the devices include network cards, ports, interfaces, power supplies, MAC addresses, SW version, OS type, CPU types, IP addresses, etc.
Address Management	Address management includes allocation IP addresses to devices, determination of subnets, keeping track of used and available IP addresses, and reuse of unused addresses. This task reduces addressing complexities and waste of address space.
Name Management	Naming establishes a connection between a name and a device, its location, its type, etc. Helps identify devices, IP address mappings, etc. Naming conventions for network devices, starting from device name to individual interface, should be planned and implemented as part of the configuration standard. A well defined naming convention provides the ability to obtain accurate information when troubleshooting. The naming convention for devices can use geographical location, building name, floor, and so forth. For the interface naming convention, it can include the segment to which a port is connected, name of connecting hub, and so forth.
Routing management	Determine and configure routing tables. This includes configuring parameters for IP routing , Quality of Service, etc.
SW distribution and upgrade	This includes detection of SW releases, distribution of new releases, and testing for interoperability.
Setting & verifying user authorization	

Activity/Service Name	*Activities/Services Provided*
Scheduling, user/flow/packet prioritization	This is to allow for a specific treatment of users, flows, or packets based on availability of features on the routers, switches and computers to meet QoS requirements or SLA's.
Resource dimensioning and allocation	Engineering the network elements for more efficient utilization and assurance to meet QoS. For example, sizing buffers.
Configuring for redundancies to assure reliability requirements	This is to design the network/systems to provide some tolerance to faults. For example, providing alternative routing, redundant computing, etc.
Initializing and terminating network operations, device reset.	This task is to initialize or shutdown the network and systems.
Setting values for fault threshold, health check intervals, performance thresholds	This task requires an enterprise manager to set and configure threshold values for the purpose of alarm monitoring and performance monitoring.
Polling for faults, health check, running watch-dog timers, processing traps	This task defines the function of either receiving or polling for alarms.
Log control	
Diagnostic testing, testing capacity and special conditions	Testing to either proactively detect a failure of some device/application/element or trying to locate faults.
fault location	Determination of fault location through testing, alarm correlation, analysis, etc.
Fault data summarization	
Reconfigure, reroute, remove Reroute	Activities to recover from fault conditions
Issue trouble ticket	Activity to document fault
Dispatch technician	
Determining the set of key performance indicators	The task of determining what performance metrics to measure. Examples are delay, response time, packet loss, buffer overlflow, etc.
Mapping SLA/user perf. objectives into network/system performance objectives	Mapping higher level service agreements such as response time, to network and system performance objectives such as processing times on each CPU, transport time, priority setting, etc.
Continuous real-time performance monitoring, performance alarm generation	Alarms, statistics, history, and host/conversation groups are used to monitor and maintain network/system availability based on application-layer traffic. Performance metrics at the interface, device, and protocol levels are collected regularly to facilitate enterprise management, capacity planning, rerouting functions The EMSs typically collect, store, and present performance data from network devices and servers. Examples of performance metrics colleted are: response time, jitter (delay variance), packet loss, input/output queuing time, input/output buffer overflow, transaction time, occupancy (utilization) of

Activity/Service Name	*Activities/Services Provided*
	resources.
Performance and statistical analysis of measured values, Performance data summarization	Post analysis of measured performance indicators for capacity planning, traffic engineering, reconfigurations, etc.
Traffic management	Determine the traffic characteristics from each source, and their resource requirements. configure the network elements, systems, to meet the requirements. User and application traffic profiling provides a detailed view of the traffic in the network. Some EMSs allow the enterprise managers to analyze and troubleshoot networked applications such as Web traffic, NetWare, Notes, e-mail, database access, Network File System (NFS),etc.
Capacity planning	Determine the traffic growth and plan for growth. Capacity planning for the network/system can be done following gathering of traffic statistics such as traffic amount and source and destination IP addresses, Input and output interface numbers, TCP/UDP source port and destination ports, source and destination of administrative groups, etc.
Establishing, maintaining and monitoring Service Level Agreements (SLA)	A service level agreement (SLA) is established between a service provider and its customer on the expected performance level of network/system services. Examples of the performance metrics used in SLA's are : guaranteed throughput, percentage of time with service availability, packet latency, percentage of packet delivery, outage reporting time, response time to denial of service attacks, service activation time, etc. Set parameters (routing, addressing, etc) in devices to meet policy requirements. Monitor operations according to the policy. Identify policy violations
Authentication and Authorization	Identify users before being allowed to access network/system resources. Authorization provides various level of authority to the user.
Accounting of Security Info	Collect and report security information used for billing, auditing, such as user identities, start and stop times, and executed commands. Accounting enables enterprise managers to track the services that users are accessing as well as the amount of network/system resources they are consuming.
Establish Access Control List	To control access of unauthorized users to network/system resources..
Policy Management, policy specification, translation and distribution.	This activity involves collection and inclusion of the various network/system related policies into the enterprise management activities. The policies include QoS, Security, Address allocation, and routing policies. A policy management tool can assist the enterprise managers in obtaining high level policies and translating them into low level policies that are to be enforced by the network devices, or *policy enforcement points*. A *policy repository* , a database of the high and low level policies, is used by these tools.
Accounting Management	Accounting management is the process used to measure network/system utilization parameters so that individual or group users on the network/system for accounting or billing. A usage-based accounting and billing system is an essential part of any service level agreement (SLA). It provides both a practical way of defining obligations under an SLA and clear consequences for behavior outside the terms of the SLA. The

Activity/Service Name	*Activities/Services Provided*
	data can be collected via NMSs. The probes to measure the statistics are places on the edge or access routers at the point of entry to the network/system. Measuring traffic flow (number of bytes, number of packets) for a specific source-destination pair (based on IP addresses). This information can also be used to check for security violations.
Specifying accounting information to be collected	
Setting and modifying accounting limits	
Defining accounting metrics	
Implementing/activating metering functions	
Controlling the storage of and access to accounting information	
Monitoring usage	
Regulating users and groups	
Billing	
Reporting	Report accounting information, configuration status, fault data, performance data , policy changes and violations

1.8 *Contracts/Regulations*

Identify any overall (human-initiated) contracts, regulations, policies, financial considerations, engineering constraints, pollution constraints, and other environmental quality issues that affect the design and requirements of the Function.

Contract/Regulation	*Impact of Contract/Regulation on Function*
SLA's between provider and user/organizations on security.	NM activities need to ensure that these SLA are met through proper network/system configuration, routing configurtion, setting and enforcing security levels if possible, determining security mechanisms, etc. Examples of SLAs are ability to access an application by only a specified set of users, ability to read or write DB, the agreement that all the communications is to be encrypted, etc.
Contracts between service providers for routing configurations.	NM activities need to ensure that the administrative boundries are set, routing agreements are met, and routing policies are enforced.

Policy	*From Actor*	*May*	*Shall Not*	*Shall*	*Description (verb)*	*To Actor*
Route Traffic	**ServiceProvider**			X	RouteTraffic	**ServiceProvider**

Contract/Regulation	*Impact of Contract/Regulation on Function*
Service Level Agreement between Network Service Provider and Users regarding performance and availability	NM activities need to ensure that these SLA are met through proper network configuration, routing configuration, setting priority levels if possible, determining alternative routes, etc. Examples of SLAs are ability to provide a throughput of *b* KBPS, ability to deliver messages of size less than *m* bytes within *t* seconds, a bound on service ability *a*% of the time, etc.

Policy	*From Actor*	*May*	*Shall Not*	*Shall*	*Description (verb)*	*To Actor*
Provide a throughput of *b* KBPS	Customer			X	Provide a throughput of *b* KBPS	ServiceProvider
Deliver messages of size less than *m* bytes within *t* seconds	Customer			x		ServiceProvider
Provide a bound on service ability *a*% of the time	Customer			x		ServiceProvider

Contract/Regulation	*Impact of Contract/Regulation on Function*
SLA's between provider and user/organizations on security.	NM activities need to ensure that these SLA are met through proper network configurtion, setting and enforcing security levels if possible, determining security mechanisms, etc.

Policy	*From Actor*	*May*	*Shall Not*	*Shall*	*Description (verb)*	*To Actor*
Limited access to an application by a specified set of users	Customer		X	X	Shall provide services to users within the set. Shall not provide services to users outside the specified list.	ServiceProvider
Encrypt all communications	Customer		x	x		ServiceProvider

Constraint	*Type*	*Description*	*Applies to*

2. Step by Step Analysis of Function

Describe steps that implement the function. If there is more than one set of steps that are relevant, make a copy of the following section grouping (Preconditions and Assumptions, Steps normal sequence, and Steps alternate or exceptional sequence, Post conditions)

2.1 Steps to implement function

Name of this sequence

2.1.1 Preconditions and Assumptions

Describe conditions that must exist prior to the initiation of the Function, such as prior state of the actors and activities

Identify any assumptions, such as what systems already exist, what contractual relations exist, and what configurations of systems are probably in place

Identify any initial states of information exchanged in the steps in the next section. For example, if a purchase order is exchanged in an activity, its precondition to the activity might be 'filled in but unapproved'.

2.1.2 Steps – Normal Sequence

Describe the normal sequence of events, focusing on steps that identify new types of information or new information exchanges or new interface issues to address. Should the sequence require detailed steps that are also used by other functions, consider creating a new "sub" function, then referring to that "subroutine" in this function. Remember that the focus should be less on the algorithms of the applications and more on the interactions and information flows between "entities", e.g. people, systems, applications, data bases, etc. There should be a direct link between the narrative and these steps.

The numbering of the sequence steps conveys the order and concurrency and iteration of the steps occur. Using a Dewey Decimal scheme, each level of nested procedure call is separated by a dot '.'. Within a level, the sequence number comprises an optional letter and an integer number. The letter specifies a concurrent sequence within the next higher level; all letter sequences are concurrent with other letter sequences. The number specifies the sequencing of messages in a given letter sequence. The absence of a letter is treated as a default 'main sequence' in parallel with the lettered sequences.

Sequence 1:

```
1.1 - Do step 1
1.2A.1 - In parallel to activity 2 B do step 1
1.2A.2 - In parallel to activity 2 B do step 2
1.2B.1 - In parallel to activity 2 A do step 1
1.2B.2 - In parallel to activity 2 A do step 2
```

1.3 - Do step 3
1.3.1 - nested step 3.1
1.3.2 - nested step 3.2

Sequence 2:

2.1 - Do step 1
2.2 – Do step 2

2.1.2.1 Performance Management

This table shows the sequence of events for performance management scenario. Step 1.5 shows an example recovery action.

#	Event	Primary Actor	Name of Process/Activity	Description of Process/Activity	Information Producer	Information Receiver	Name of Info Exchanged	Additional Notes	IECSA Environments
#	*Triggering event: Identify the name of the event.*[2]	*What other actors are primarily responsible for the Process/Activity. Actors are defined in section1.5.*	*Label that would appear in a process diagram. Use action verbs when naming activity.*	*Describe the actions that take place in active and present tense. The step should be a descriptive noun/verb phrase that portrays an outline summary of the step. "If …Then…Else" scenarios can be captured as multiple Actions or as separate steps.*	*What other actors are primarily responsible for Producing the information.Actors are defined in section1.5.*	*What other actors are primarily responsible for Receiving the information Actors are defined in section1.5.* *(Note – May leave blank if same as Primary Actor)*	*Name of the information object. Information objects are defined in section 1.6*	*Elaborate architectural issues using attached spreadsheet. Use this column to elaborate details that aren't captured in the spreadsheet.*	*Reference the applicable IECSA Environment containing this data exchange. Only one environment per step.*
1.1		EnterpriseManager	Get Performance Data	NMS manager requests performance data.	EnterpriseManager	EnergyManagementSystem	GetRequest		Control Center / Corporations
1.2		EnergyManagementSystem	Get Performance Data	EnergyManagementSystem polls data from manageddevice	EnergyManagementSystem	ManagedDevice	GetRequest		Intra-Control Center

[2] Note – A triggering event is not necessary if the completion of the prior step leads to the transition of the following step.

#	Event	Primary Actor	Name of Process/Activity	Description of Process/Activity	Information Producer	Information Receiver	Name of Info Exchanged	Additional Notes	IECSA Environments
1.3		ManagedDevice	Provide performanceData	EnergyManagementSystem gets data from manageddevice	ManagedDevice	EnergyManagementSystem	PerformanceData		Intra-Control Center
1.4		EnergyManagementSystem	Post Results on Management Client	Post results	EnergyManagementSystem	EnterpriseManager	PerformanceData		Control Center / Corporations
1.5		EnterpriseManager	Change Configuration	The manager detects problem, find a solution, that may affect the same or another managed device	EnterpriseManager	EnergyManagementSystem	Configuration Data	If no problem is identified, the function stops.	Control Center / Corporations
1.6		EnergyManagementSystem	Change Configuration	EnergyManagementSystem passes the configuration data to the device in the proper format.	EnergyManagementSystem	ManagedDevice2	Configuration Data		Intra-Control Center

2.1.1 Post-conditions and Significant Results

Describe conditions that must exist at the conclusion of the Function. Identify significant items similar to that in the preconditions section.

Describe any significant results from the Function

Actor/Activity	*Post-conditions Description and Results*

2.2 *Architectural Issues in Interactions*

Elaborate on all architectural issues in each of the steps outlined in each of the sequences above. Reference the Step by number..

Microsoft Excel Worksheet

3. Auxiliary Issues

3.1 *References and Contacts*

Documents and individuals or organizations used as background to the function described; other functions referenced by this function, or acting as "sub" functions; or other documentation that clarifies the requirements or activities described. All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work must be so noted.

[ATMF 94] ATM Forum, "Customer Network Management (CNM) for ATM Public Network Service," ATMF Specification af-nm-0019.000, Oct, 1994

[ATMF 96] ATM Forum, "Integrated Local Mgmt. Interface (ILMI) Ver. 4.0," ATMF Specification af-ilmi-0065.000, Sep, 1996.

[ATMF 97] ATM Forum, "ATM Remote Monitoring SNMP MIB," ATMF Specification af-nm-test-0080.000, July 1997

[ATMF 98] ATM Forum, "SNMP M4 Network Element View MIB," ATMF Specification af-nm-0095.001, July 1998

[ATMF 99a] ATM Forum, "Network Management M4 Security Requirements and Logical MIB," ATMF Specification af-nm-0103.000, Jan, 1999

[ATMF 99b] ATM Forum, "M4 Interface Requirements and Logical MIB: ATM Network View Version 2," ATMF Specification af-nm-0058.001, May, 1999

[ATMF 99c] ATM Forum, "Auto-configuration of PVCs Specification," ATMF Specification af-nm-0122.000, May 1999

[ATMF 99d] ATM Forum, "CMIP Specification for the M4 Interface: ATM Network Element View, Version 2," ATMF Specification af-nm-0027.001, July, 1999

[ATMF 00] ATM Forum, "ATM Usage Measurement Requirements," ATMF Specification af-nm-0154.000, November 2000

ATMF 01a] ATM Forum, "Requirements and Logical MIB for Management of Path and Connection Trace," ATMF Specification, af-nm-0153.000, April, 2001

[ATMF 01b] ATM Forum, "CORBA Specification for M4 Interface: Network View", ATMF Letter Ballot Document: fb-nm-0166.000, Apr 2001.

[ATMF 02] ATM Forum, "M4 Interface: ATM Network View, CORBA MIB, Version 2," ATMF Specification af-nm-0185.000, August, 2002

[ATMF 03] ATM Forum, "ATM Performance Management Bulk, Data File Structure," ATMF Specification af-nm-0194.000, April, 2003

[Bell 93] Bellcore TA-NWT-001114, Generic Requirements for Operations Interfaces Using OSI Tools: ATM/Broadband Network Management, Issue 2, October 1993.

[Bell 96] GR-2869-CORE, *Generic Requirements for Operations Based on the Telecommunications Management Network (TMN) Architectur*e, Issue 2, Bellcore, October 1996.

[Bell 94] SR-TSV-002690, *Requirements for an EML Platform Environment*, Bellcore, Issue 1, March 1994.

[Bell 96] *Network Management Layer to Element Manager Interface Descriptio*n, Bellcore, February 1996.

[Bell 00] Bellavista P., Corradi A., Stefanelli C., "An Integrated Management Environment for Network Resources and Services," IEEE Journal on Selected Areas in Communications, Vol. 18, No. 5, May 2000

[Casa 00] Casassa M., Baldwin A., Goh C., "POWER Prototype: Towards Integrated Policy-Based Management," IEEE/IFIP Network Operations and Management Symposium, 2000.
[Chei 98] Cheikhrouhou M. M., Conti P., Labetoulle J., "Intelligent Agents in Network Management: A State-of-the-art," 1998
[CORBA] CORBA www.omg.org, www.corba.org
[Dobs 89] Dobson J.E., McDermid J.A.,"A Framework for Expressing Models of Security Policy," IEEE Symposium on Security & Privacy, May 1989, Oakland, CA, 1989.
[DOCS OSSI] Data-Over-Cable Service Interface Specifications DOCSIS 2.0 - Operations Support System Interface Specification, SP-OSSIv2.0-104-030730, July 2003.
[DSLF TR005] DSL Forum "ADSL Network Element Management", DSL Forum Technical Report TR-005, March 1998.
[DSLF TR022] DSL Forum, "The Operation of ADSL-based Networks," DSL Forum Technical Report TR-022, August 1999.
[DSLF TR030] DSL Forum, "ADSL EMS to NMS Functional Requirements," DSL Forum Technical Report TR-030, Feb 2000.
[DSLF TR035] DSL Forum, "Protocol Independent Object Model for ADSL EMS-NMS Interface," DSL Forum Technical Report: TR-035, March 2000.
[DSLF TR041] DSL Forum, "CORBA Specification for ADSL EMS-NMS Interface," DSLF Technical Report TR-041, June 2001.
[DSLF TR046] DSL Forum, "Auto-Configuration Architecture & Framework", DSL Forum Technical Report, TR-046, February 2002.
[Enns 03] R. Enns, "XMLCONF Cofiguration Protocol", IETF Internet Draft draft-enns-xmlconf-spec-00.txt, Feb. 2003.
[Gins 99a] D. Ginsburg, *ATM Solutions for Enterprise Internetworking, 2nd Edition*, Addison Wesley, 1999.
[Gins 99b] D. Ginsbury, Implementing *ADSL*, Addison Wesley, 1999.
[Gold 95] Goldszmidt G., Yemini Y., "Distributed Management by Delegation," Procs. Of the 15th International Conference on Distributed Computing Systems, June 1995
[Hege 99] Hegering H., Abeck S., Neumair B., *Integrated Management of Network Systems*, Morgan Kaufmann Publishers, Inc. 1999
[IEEE] IEEE www.ieee.org
[IETF] IETF www.ietf.org.
[IPDR 02] "Network Data Management – Usage (NDM-U) For IP-Based Services", Version 3.1, IPDR.org, April 15, 2002.
[ISO] ISO www.iso.ch
[ITU G9971] ITU-T Draft Recommendation G.997.1, "Physical Layer Management for Digital Subscriber Line (DSL) Transceivers", October 1998.
[ITU M3010] ITU-T Recommendation M.3010: "Principles for a Telecommunications Management Network", October 1992.
[ITU M3100] ITU-T Recommendation M.3100: "Generic Network Information Model Version 2", March 1995.
[ITU M3120] ITU-T, SG4, Recommendation M.3120, "CORBA Generic Network and NE Level Information Model," October 2001.
[ITU Q8221] ITU-T, SG4, Recommendation Q.822.1, "CORBA-based TMN Performance Management Service", October 2001.
[ITU X720] ITU-T Recommendation X.720, "Information Technology – Open Systems Interconnection – Structure of Management Information: Management Information Model," January 1992.
[ITU X721] ITU-T Recommendation X.721, "Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information", February 1992.
[JMX] JMX www.java.com

[Ju 01] Ju H., Choi M., Hong J., "EWS-Based Management Application Interface and Integration Mechanisms for Web-Based Element Management," Journal of Network and Systems Management, Vol.9, No.1, 2001
[Knig 99] Knight G., Hazemi R., "Mobile Agent-Based Management in the INSERT Project," Journal on Network and Systems Management, Vol.7, 1999
[Koch 01] Koch F. L., Westphall C. B., "Decentralized Network Management Using Distributed Artificial Intelligence," Journal of Network and Systems Management, Vol.9, No.4, Dec. 2001
[Lang 97] Lange, D., "Java Aglets Application Programming Interface (J-AAPI)," IBM white paper, Feb. 1997. (www.trl.ibm.com/aglets/JAAPI-whitepaper.htm)
[Lupu 99] Lupu E., Sloman M., "Conflicts in Policy-Based Distributed Systems Management," IEEE Transactions on Software Engineering, Vol. 25, No. 6, Nov. 1999.
[Mani 00] Subramanian, Mani, *Network Management, Principles and Practice*, Addison Wesley, 2000.
[Mart 98] Martin-Flatin J., "Push vs. Pull in Web-Based Network Management, "Technical Report SSC/1998/002, Swiss Federal Institute of Technology Lausanne, 1998
[Mart 99] Martin-Flatin J. P., Znaty S., Hubaux J. P., "A Survey of Distributed Enterprise Network and Systems Management Paradigms," Journal of Network and Systems Management, Vol.7, No.1, 1999
[Moff 93] Moffett J., Sloman M., Policy Hierarchies for Distributed Systems Management, IEEE Journal on Selected Areas in Communication, Vol. 11, No. 9, Dec. 1993.
[Nade 03] T. D. Nadeau, *MPLS Network Management - MIBs, Tools and Techniques*, Morgan Kaufmann, 2003.
[OMG 99] The Object Management Group (OMG), "The Common Object Request Broker: Architecture and Specification", OMG Document: formal/99-10-07, Revision 2.3.1, October 1999.
[Proz 97] Prozeller P., "TINA and the Software Infrastructure of the Telecom Network of the Future," Journal on Network and System Management, Vol.5, Dec. 1997
[Raou 02] Raouf Boutaba, Jin Xiao, "Network Management: State of the Art," Communication Systems: The State of the Art (IFIP World Computer Congress), p.g.127-146, 2002.
[RFC 1155] K. McCloghrie, M. Rose, "Structure and Identification of Management Information for TCP/IP-based Internets," IETF RFC 1155, May 1990.
[RFC 1157] Schoffstall, M., Fedor, M., Davin, J. and Case, J., A Simple Network Management Protocol (SNMP), IETF RFC 1157, May, 1990
[RFC 1212] K. McCloghrie, M. Rose, "Concise MIB Definitions", IETF RFC 1212, March, 1991.
[RFC 1213] K. McCloghrie and M. Rose. Management Information Base for Network Management of TCP/IP-base Internets: MIB-II, IETF RFC 1213, and March 1991
[RFC 1215] Rose, M.T. "A Convention for Defining Traps for use with the SNMP", IETF RFC 1215, March 1991.
[RFC 1224] L. Steinberg. Techniques for Managing Asynchronously Generated Alerts, IETF RFC 1224, May, 1991
[RFC 1406] F. Baker, J. Watt, "Definitions of Managed Objects for the DS1 and E1 Interface Types", IETF RFC 1406, Jan 1993.
[RFC 1407] T. Cox, K. Tesink, "Definitions of Managed Objects for the DS3/E3 Interface Type", IETF RFC 1407, Jan 1993.
[RFC 1441] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Introduction to version 2 of the Internet-standard Network Management Framework", IETF RFC 1441, May 1993.

[RFC 1442] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1442, May 1993.
[RFC 1443] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1443, May 1993.
[RFC 1444] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1444, May 1993.
[RFC 1445] J. Davin, K. McCloghrie, "Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1445, May 1993.
[RFC 1446] J. Galvin, K. McCloghrie, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1446, May 1993.
[RFC 1447] K. McCloghrie, J. Galvin, "Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1447, May 1993.
[RFC 1448] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1448, May 1993.
[RFC 1449] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1449, May 1993.
[RFC 1450] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1450, May 1993.
[RFC 1451] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Manager to Manager Management Information Base", IETF RFC 1451, May, 1993.
[RFC 1452] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework", IETF RFC 1452, May 1993.
[RFC 1493] E. Decker, P. Langille, A. Rijsinghani, and K.McCloghrie., Definitions of Managed Objects for Bridges, IETF RFC 1493, July, 1993
[RFC 1573] K. McCloghrie, F. Kastenholz, "Evolution of the Interfaces Group of MIB-II", IETF RFC 1573, Jan 1994.
[RFC 1595] T. Brown, K. Tesink, "Definitions of Managed Objects for the SONET/SDH Interface Type", IETF RFC 1595, March 1994.
[RFC 1695] M. Ahmed and K. Tesink, "Definitions of Managed Objects for ATM Management, Version 8.0 using SMIv2", IETF RFC 1695, August 1994.
[RFC 1757] Waldbusser S., Remote Network Monitoring Management Information Base., IETF RFC 1757, Feb. 1995
[RFC 1901] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Introduction to Community-based SNMPv2", IETF RFC 1901, January 1996.
[RFC 1903] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1903, January 1996.
[RFC 1905] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1905, January 1996.
[RFC 1906] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", IETF RFC 1906, January 1996

[RFC 1907] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, “Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)”, IETF RFC 1907, January 1996.
[RFC 2011] K. McCloghrie, “Category: Standards Track SNMPv2 Management Information Base for the Internet Protocol using SMIv2”, IETF RFC 2011, November 1996
[RFC 2013] K. McCloghrie, “Category: Standards Track SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2”, IETF RFC 2013, November 1996
[RFC 2570] J. Case, R. Mundy, D. Partain, B. Stewart, “Introduction to Version 3 of the Internet-standard Network Management Framework”, IETF RFC 2570, April 1999
[RFC 2571] Harrington, D., Presuhn, R. and B. Wijnen, “An Architecture for Describing SNMP Management Frameworks”, IETF RFC 2571, April 1999.
[RFC 2572] Case, J., Harrington, D., Presuhn, R. and B. Wijnen, “Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)”, IETF RFC 2572, April 1999
[RFC 2573] Levi, D., Meyer, P. and B. Stewart, “SNMP Applications”, IETF RFC 2573, April 1999.
[RFC 2574] Blumenthal, U. and B. Wijnen, “The User-Based Security Model for Version 3 of the Simple Network Management Protocol (SNMPv3)”, IETF RFC 2574, April 1999
[RFC 2575] Wijnen, B., Presuhn, R. and K. McCloghrie, “View-based Access Control Model for the Simple Network Management Protocol (SNMP)”, IETF RFC 2575, April 1999
[RFC 2576] R. Frye, D. Levi, S. Routhier, B. Wijnen, “Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard and Network Management Framework”, IETF RFC 2576, March 2000.
[RFC 2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, “Structure of Management Information Version 2 (SMIv2)”, IETF RFC 2578, April 1999
[RFC 2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, “Textual Conventions for SMIv2”, IETF RFC 2579, April 1999
[RFC 2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, “Conformance Statements for SMIv2”, IETF RFC 2580, April 1999
[RFC 2662] B. Bathrick, F. Ly, "Definitions of Managed Objects for the ADSL Lines", IETF RFC 2662, August 1999.
[RFC 2665] J. Flick, J. Johnson, “Definitions of Managed Objects for the Ethernet-like Interface Types”, August 1999
[RFC 2669] M. St. Johns, “DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems”, August 1999
[RFC 2670] M. St. Johns, “Radio Frequency (RF) Interface Management Information Base for MCNS DOCSIS compliant RF interfaces”, August 1999
[RFC 2748] D. Durham, Ed. "The COPS (Common Open Policy Service) Protocol," IETF RFC 2748, Jan. 2000.
[RFC 2786] M. St. Johns, “Diffie-Helman USM Key Management Information Base and Textual Convention”, IETF RFC 2786, Aug, 1999
[RFC 2863] K. McCloghrie, F. Kastenholz, “The Interfaces Group MIB”, June 2000.
[RFC 2933] McCloghrie, K., Farinacci, D., Thaler, D., “Internet Group Management Protocol MIB”, IETF RFC 2933

[RFC 3083] R. Woundy, “Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems”, RFC 3083, March 2001.
[RFC 3084] Chan K, et al, "COPS Usage for Policy Provisioning," IETF RFC 3084, March 2001.
[RFC 3483] D. Rawlins et al, "Framework for Policy Usage Feedback for Common Open Policy Service with Policy Provisioning (COPS-PR)," March 2003.
[Roge 02] Rogerson D., Inside COM, Redmond, WA, Microsoft, 1997
[Stra 96] Straber M., Baumann J., Fohl F., "Mole – A Java Based Mobile Agent System," 10th European Conference on Object-Oriented Programming ECOOP’96. Jul. 1996
[Thom 98] Thompson J., "Web-based Enterprise Management Architecture," IEEE Communications Magazine, Mar. 1998
[WBEM] www.dmtf.org
[Wool 95] Wooldridge M., Jennings N. R., "Intelligent Agents: Theory and Practice, The Knowledge Engineering Review," Vol. 10, No.2, 1995

3.2 *Action Item List*

As the function is developed, identify issues that still need clarification, resolution, or other notice taken of them. This can act as an Action Item list.

ID	Description	Status

3.3 *Revision History*

For reference and tracking purposes, indicate who worked on describing this function, and what aspect they undertook.

No	Date	Author	Description
01.			

This page intentionally left blank.