ELECTRIC POWER
RESEARCH INSTITUTE

Network Security Management for Transmission Systems

1024421

Network Security Management for Transmission Systems

1024421

Technical Update, December 2012

EPRI Project Manager

G. Rasche

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

IAP Solutions

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

IAP Solutions
303 Twin Dolphin Drive, Suite 600
Redwood City, CA 94065

Principal Investigator
D. Gosch

This report describes research sponsored by EPRI.

The author wishes to acknowledge the consulting expertise provided by:

JDS Management Software – J. Saperia

NCI Security – S. Bromberger

Utility Ethernet Forum – T. Janca

Xanthus Consulting – F. Cleveland

This publication is a corporate document that should be cited in the literature in the following manner:

Network Security Management for Transmission Systems. EPRI, Palo Alto, CA: 2012. 1024421.

ABSTRACT

The electric power grid is increasingly dependent on information technology and telecommunication infrastructures. While great benefits will result from this influx of technology, a holistic and granular awareness of all elements of the information infrastructure supporting a control subsystem will be critical to ensure long term reliability and security. The management of this information infrastructure requires connectivity and analytics to support both IT and OT assets in a unified manner.

The objective of this report is to identify where network and system management (NSM) standards/technology are applicable and valuable to the bulk electric transmission system for enhanced wide area situational awareness, security, reliability and system confidence as network intelligence advances. It provides several “Use Cases” that are intended to identify the actors and objectives of a system’s solution set and to generate utility and vendor input on the challenges being tackled, solutions being addressed and effectiveness of the standardized solution work proposed. Given the increasing level of automation and Information and Communication Technologies (ICT) being deployed within the bulk electrical system, it is also necessary to discuss at a high level how new intelligence creates unforeseen challenges to grid operations which would be addressed by an NSM standard. Additionally, the International Electrotechnical Commission (IEC) 62351-7 standard for common information security objects is reviewed with feedback provided for the IEC Technical Committee (TC) 57 Working Group (WG) 15.

Finally, a series of next steps are proposed, with the objective of achieving a comprehensive use case based approach targeting the domain of substation control networks and other high-priority architectures. A key result will be the identification of additional monitoring objects for more advanced awareness of network and power devices, supporting the system’s ability to resolve root-cause issues with minimal human interaction or to provide a complete picture for effective human decision making. Some technologies such as multiservice communications using switched packet methods (i.e. Multiprotocol Label Switching) will require additional details of configuration and service level expectations in order to offer complete monitoring capabilities.

Keywords
Network Management System
IEC 62351-7
Security Object Model
Cyber Security

EXECUTIVE SUMMARY

Power systems operations are increasingly reliant on information infrastructures, including communication networks, intelligent electronic devices (IEDs), and self-defining communication protocols [1]. Therefore, management of the information infrastructure is crucial to providing the necessary high levels of security and reliability in power system operations. Until recently, communications and information flows have been considered of peripheral importance. However, increasingly the information infrastructure that supports the monitoring and control of the power system has been recognized to be critical to the reliability and security of the power system.

The objective of this report is to identify where network and system management (NSM) standards/technology are applicable and valuable to the bulk electric transmission system for enhanced situational awareness, security, reliability and system confidence as network intelligence advances. Having a holistic and granular awareness of all elements of the information infrastructure supporting control subsystems will be critical to supporting long term reliability and security. In the long-term, this effort seeks to promote a common set of information objects to manage networks, security, and end devices. This research effort is also engaged with the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 to promote the standardization and interoperability of these objects.

This project provides a set of NSM use cases, resulting requirements and a review of the IEC 62351-7 standard. A demonstration trial has also been implemented to show the end-to-end functionality of a Network and System Manager.

The next stage requires the formalization of this approach within a specific domain of market priority, which can then be duplicated and expanded to additional scenarios and domains. A conceptual model of next steps is included in this report which will result in prototype implementations, including protocol-specific extensions for information security objects.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 APPROACH

The evolving electric sector is increasingly dependent upon information technology and telecommunications infrastructures to enable new capabilities for improved efficiency, increased reliability and the integration of renewable energy. Ensuring the reliability and security of the electrical grid also requires proper management of this rapidly growing information infrastructure in a comprehensive manner.

The IEC TC57 WG 15 began to address this challenge by developing a group of common information security objects, which is an abstract data model for management of the power systems information infrastructure. Their recommendation was that common objects will facilitate a standardized approach for continued robustness as well as enable interoperability between vendors. These objects are defined in the IEC 62351-7 standard, which subsequently identifies this emerging sector as Network and System Management (NSM).

The Telecommunications industry has achieved similar results through the operations support of evolving and converging networking technologies, using the ISO Telecommunications management model with Fault, Configuration, Accounting, Performance, Security (FCAPS) based management systems. The results show improved overall system reliability, security as well continual improvements in operational efficiency. This capability is an enabler for breaking down solution silos over time, a growing objective within several smart grid architecture organizations.

Document Objective

The objective of this report is to identify where network and system management (NSM) standards/technology are applicable and valuable to the bulk electric transmission system for enhanced wide area situational awareness, security, reliability and system confidence as network intelligence advances. It provides several “Use Cases” that are intended to identify the actors and objectives of a system’s solution set and to generate utility and vendor input on the challenges being tackled, solutions being addressed and effectiveness of the standardized solution work proposed. Given the increasing level of automation and Information and Communication Technologies (ICT) being deployed within the bulk electrical system, it is also necessary to discuss at a high level how new intelligence creates unforeseen challenges to grid operations which would be addressed by an NSM standard. Additionally, the International Electrotechnical Commission (IEC) 62351-7 standard for common information security objects is reviewed with feedback provided for the IEC Technical Committee (TC) 57 Working Group (WG) 15.

Finally, a series of next steps are proposed, with the objective of achieving a comprehensive use case based approach targeting the domain of substation control networks and other high-priority architectures. A key result will be the identification of additional monitoring objects for more advanced awareness of network and power devices, supporting the system’s ability to resolve root-cause issues with minimal human interaction or to provide a complete picture for effective human decision making. Some technologies such as multiservice communications using switched packet methods (i.e. Multiprotocol Label Switching) will require additional details of configuration and service level expectations in order to offer complete monitoring capabilities.

Approach

Since this problem space touches a variety of technical topics, a team was assembled containing subject matter experts in the areas of telecommunications management, electrical transmission control communications, and cyber security practice as related to the utility industry. The core team's initial results have been provided for review to a larger circle consisting of:

- EPRI P183 cyber security team
- NESCOR Team 2
- Select major utilities
- Vendors focused on security practice and products

In parallel, EPRI implemented an end-to-end trial demonstrating a single use case scenario based upon a security breach of a substation yard, as well as the substation LAN. This was implemented from an NMS using both an existing proprietary data model as well as a parallel implementation based upon IEC 62351-7.

Regardless of implementation of methods currently available, one of the most important outcomes is the exposure of network and system management as often overlooked with initial IP communications deployments within power systems. The establishment of a knowledge base and requirements methodology which can be extended to all T&D domains is also of prime importance for the next project stage.

IEC 62351-7 NSM Introduction

The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Power Systems Management and Associated Information Exchange is responsible for developing international standards for power system information exchanges. Its scope is:

> *"To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems and databases, which may be outside the scope of TC 57 [2]."*

IEC TC57 has developed five widely accepted communication standards, and has been the source of a sixth. These protocols are:

- IEC 60870-5: Widely used in Europe and other non-US countries for SCADA system to RTU data communications. It is used both in serial links (Part 101) and over networks (Part 104).

- DNP 3 (IEEE 1815): Derived from IEC 60870-5 and in use in North America and in many other countries as well, primarily for SCADA system to RTU data communications.

- IEC 60870-6 (also known as TASE.2 or ICCP): Used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers.

- IEC 61850: Used for interactions with field equipment, including protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control center, and other power industry operational functions. It also includes profiles to meet the ultra fast response times of protective relaying and for the sampling of measured values.

- IEC 61968 and IEC 61970 (Common Information Model CIM): Used for application-to-application interactions, primarily within utility operations centers. It consists of a UML abstract model of the power system and includes information models and messaging for application-level information exchanges for transmission, distribution, and market functions.

- IEC 61334 (DLMS): Used for retrieving metering information and managing meter settings, primarily outside of North America.

This architecture of TC57 information exchange standards [3] is illustrated in Figure 1-1.

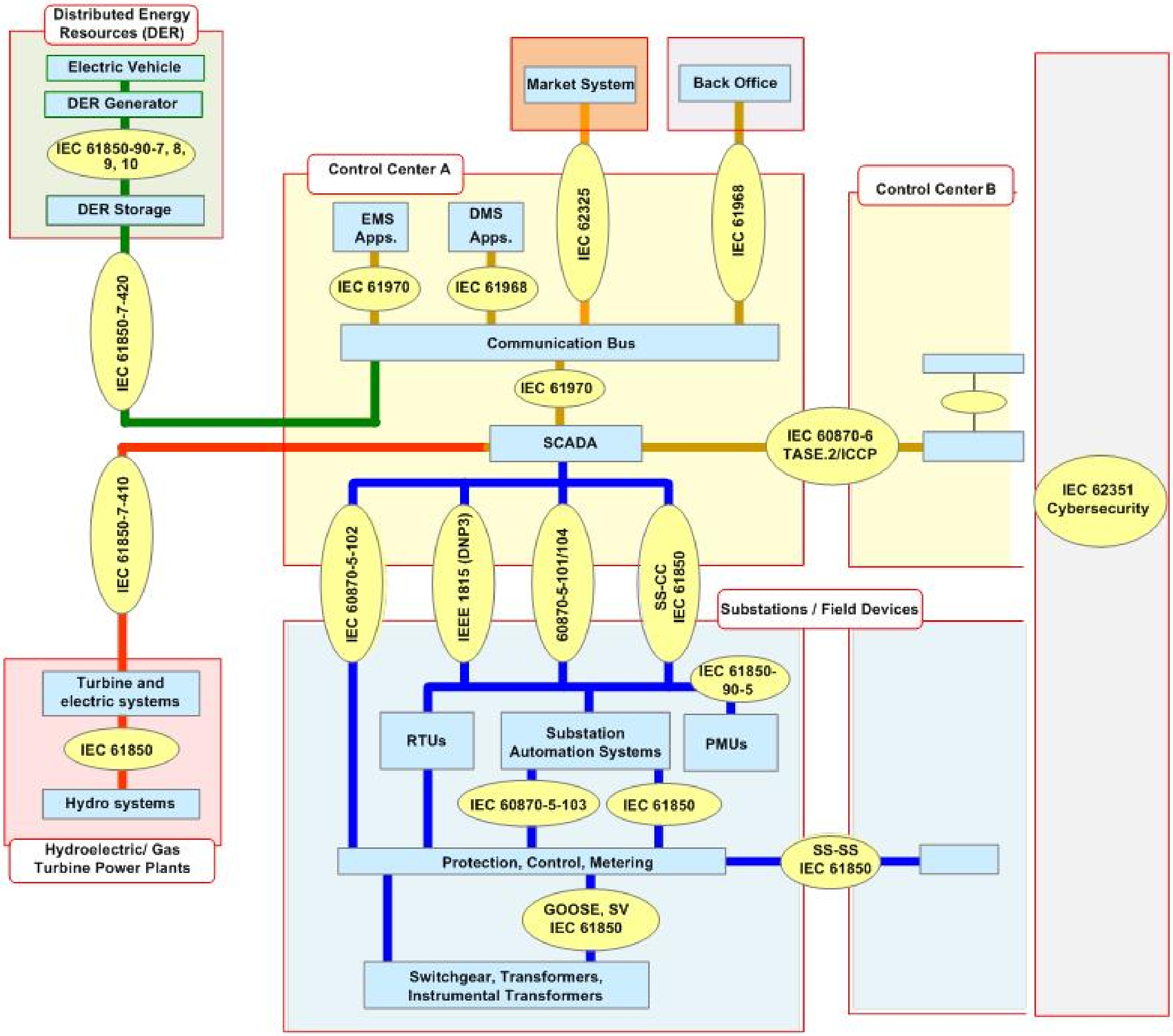


Figure 1-1
Architecture of IEC TC57 Information Exchange Standards

The reliability of the power system is increasingly affected by any problems that the information infrastructure might suffer, and therefore the information infrastructure must be managed to the level of reliability needed to provide the required reliability of the power system infrastructure.

IEC 62351-7 is the 7th part of the IEC 62351 Security Standards from the IEC TC57 WG15 [1]. Figure 1-2 shows how the IEC electrical and network system standards map to one another. Secure utility architectures are tightly linked with network architecture choices, network paradigms and the ability to structure network system management information in a meaningful and effective manner for system actors. The goal of IEC 62351-7 is to establish standardized network object models to facilitate interoperability for ICT management for all the networks shown in Figure 1-2.

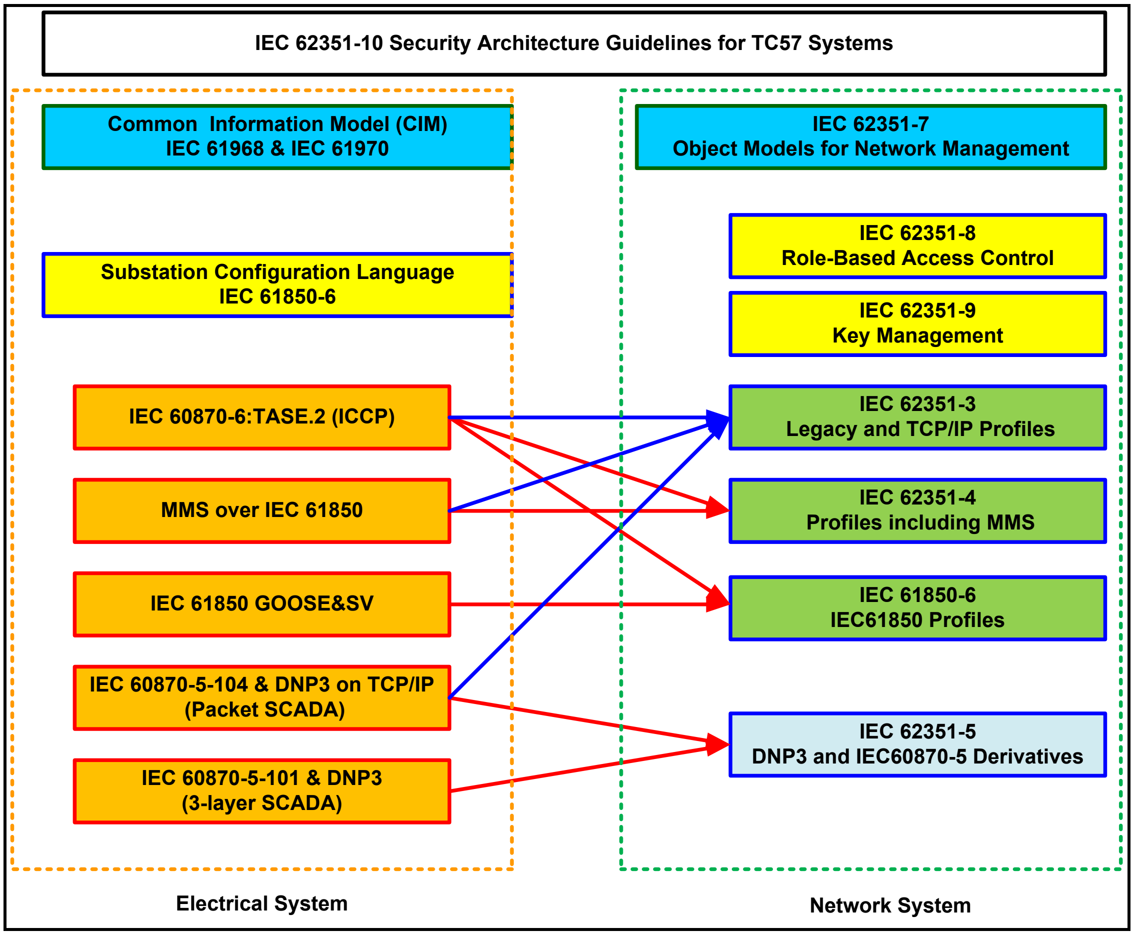

IEC 62351-10 Security Architecture Guidelines for TC57 Systems
Common Information Model (CIM)
IEC 61968 & IEC 61970
Substation Configuration Language
IEC 61850-6
IEC 60870-6:TASE.2 (ICCP)
MMS over IEC 61850
IEC 61850 GOOSE&SV
IEC 60870-5-104 & DNP3 on TCP/IP
(Packet SCADA)
IEC 60870-5-101 & DNP3
(3-layer SCADA)
IEC 62351-7
Object Models for Network Management
IEC 62351-8
Role-Based Access Control
IEC 62351-9
Key Management
IEC 62351-3
Legacy and TCP/IP Profiles
IEC 62351-4
Profiles including MMS
IEC 61850-6
IEC61850 Profiles
IEC 62351-5
DNP3 and IEC60870-5 Derivatives
Electrical System
Network System

Figure 1-2
Interrelationships Between the IEC TC57 Standards and the IEC 62351 Security Standards

IEC 62351-7 Edition 1 standard provides a first draft of abstract object models for performing interoperable network and system management functions to enable security architecture guidelines advancing secure access, reliability and network confidence. NSM standard object models will enhance the actors' ability to know the networks' logical and physical state while increasing awareness of how network messaging health is impacting the automation, control and protection of a bulk electrical system.

NSM objects would be implemented in communication network channels and nodes allowing network and system security and performance to be monitored, protected and controlled. NSM objects would leverage and extend existing network control and management protocol standards while creating utility centric standardized object models that are interoperable across various equipment vendors for bulk power system automation and information systems.

NSM objects embedded in network node devices and intelligent electronic devices would provide an interoperable informational model allowing independent or integrated awareness of network activity, state and health within utility networks. Network devices would support network-time visibility, enhancing maintenance and management capabilities.

The NSM standard is intended to be implemented in all areas of power system management. However, this report starts with Transmission Substation Automation devices, including Substation

Gateways, Communication Processors, Remote Terminal Units (RTU) and other network terminal (Data Terminal Equipment (DTE) or Intelligent Electronic Devices (IED)) and communication (DCE or Network Element) devices. The information objects are used by the Network Management Systems (NMS) and the utility's System Information and Event Manager (SIEM) to coordinate monitoring and action.

2
TRANSMISSION SYSTEMS

Power flow monitoring, protection and control within transmission substations is accomplished through the use of local and regionally distributed networks that are diverse in technology, age and architecture. Utility networks have historically been hierarchical master/slave or client/server information networks with traditional protocols. However, protocols like IEC 61850 are disrupting the classical utility information network model by enabling networks of intelligent devices to publish and subscribe to system measurements and states. This approach allows systems to coordinate optimization, operation and protection through the use of packet-based networks. However, advanced protection, automation and control applications require ICT architectures and technology implementations that provide confidence, security, reliability, and determinism in network operations.

Applying Network and System Management to Transmission Systems

Network and System Management is a collection of functions which can be implemented by various elements within a transmission system to meet these key objectives:

1. Functional and non-functional operational status of the network, channels, links and ports
2. Uniform and logically consistent packet prioritization, service segmentation, and processing internally (SLAN) and externally (SSAN, SWAN)
3. Electronic security perimeter establishment, authentication and traffic control

The primary objective of Network & System Management is to assist actors (intelligent devices, human operators and engineers) to gain intelligent information on the functional and non-functional performance of the devices' network services in network-time[1]. Utility networks are becoming more packet-centric where non-functional requirements (data rates, throughput, latency, dependability and security) are more often logically configured than hardware defined. This approach increases flexibility and capabilities at the risk of less deterministic performance. However, the time sensitive nature of measurands, command states, and action messages make the traditionally "non-functional" requirements imperative to an electrical system's decision, action, and restraint functions.

NSM's secondary objective is to ensure and enhance uniform logical configuration of network elements and to provide visibility into the activity on the network. Information about the virtual tunnels, label switched paths, and packet priorities (both internal to the transmission utility network and where communication links are established with 3rd party actors within the system) can be used to ensure symmetrical traffic processing on critical packets. While SCADA, ICCP and teleprotection are among the higher level functional silos within transmission substations, they are converging as protocols emerge which integrate and enable both reporting and protection

[1] Network-time refers to the maximum update information rate on network status by the limiting line rate of the network(s) providing NSM data to central or distributed network operation centers.

functions within an intelligent device through a common or redundant gateway. IEC 61850-8 and IEC 61850-9 services extend the ability through Ethernet to publish and subscribe to analog and digital values amongst multiple stations, enhancing wide area monitoring and protection capabilities through the 61850 gateway and replacing the traditional RTU. Time sensitive messaging like protective relaying trip and blocking commands along with power flow measurements and derived values become transported and integrated through common gateways whose logical configuration and technology choices set deterministic performance and security.

NSM's third objective is to effectively monitor, maintain, and secure the electronic security perimeter for the substation networks and their connectivity to external networks in a way that meets regulatory and utility security requirements. Transmission substations are the demarcation ingress point in the bulk electrical system with their regional transmission distances serving distribution tier stations, 3rd-party bulk distributed energy resources (DER) and wide area monitoring and control connectivity to extranets. Increasing security while expanding access at the transmission exchange is vital to improving regional access to critical operational information. A standardized NSM system would enhance the network-time ability to monitor, segment and secure information external to the transmission utilities' Operation-Safety-Enterprise network functions while being interoperable between different systems and users. Periodic audits of electronic security perimeters could also be enhanced by NSM monitoring and enforcing perimeter services adding to the compliance value of such systems.

Utility Network Message Types and Priorities

Intelligent utility networks rely on messaging to discern the state and condition of the electrical network and take appropriate action to ensure stability and reliability of electrical power flow. As Substation LAN ICT replaces hard contact connectivity, the importance of local station ICT system health, performance and security increases. Advancing wide area situational awareness through ICT and moving to the application of real-time analytics in automation functions requires awareness of traffic flows, message time and synchronization of network state.

Power system messages can be categorized as status, alarms, measurements, commands, records, and logs that serve the system's operational and maintenance functions of protection, control and instrumentation. The message type and function determines the handling and prioritization of the message within the network structure. The substation LAN gateway is responsible for the correct prioritization, security, segmentation, and reliability of the critical and non-critical messaging within the substation LAN (SLAN) and substation wide area network (SWAN). Protective relays manage their internal interactions over the Process Bus and their external interactions with other protective relays in circuit associated substations via the substation-substation area network (SSAN).

NSM within transmission tier substations would provide visibility into the SLAN messaging types and functions by creating terminal and node monitoring points that measure message performance. The NSM may also have significant value across regional transmission substations in the SSAN and SWAN utility network, where it can provide visibility, security, control and performance supervision of the Substation Gateway to the utility substation networks and control centers.

Utility Network Message Timing Effects

Network latency induced phase/time errors will rise in importance as transmission electrical circuits migrate to more networked electric circuits incorporating DER and redundant sources and lines. Currently, the primary focus is on teleprotection with centralized generation. However, emerging applications that integrate networked generation sources automatically will benefit from known network message transit times. Since operational control is achieved through combinational and sequential logic driven by analog inputs that engage and disengage generator sources, load shedding and balancing actions must all occur at the proper time. NSM objects could provide the time accounting information to improve the action resolution of protection and control operations across interconnected grids.

Transmission line protection communication is often high-priority, direct-zone communication between substations using pilot tones, power line carrier, microwave, direct or multiplexed fiber optics and may require redundant communication paths. Line teleprotection schemes can be a blend of command or comparison and occur autonomously based on directly measured values or compared values as in line differential protection. Time skews in high-speed relays have sensitivities to asymmetrical path transit times which can occur between required primary and secondary paths utilizing different media (microwave and fiber optics). NSM objects provide value in high-speed relaying communication channels by measuring, reporting and controlling path latencies. Additionally, an NSM system can inform the actor what the messaging time is of a given logical channel service, allowing the message delivery time to move from an “unknown” variable to a “known” variable when taking real time action or analyzing forensic events. Increasing awareness of the message processing and delivery times enhances system intelligence where critical automation systems are impacted by messaging time skews.

3
USE CASES

Network security emerges from a disciplined, well-defined utility network architecture whose guiding principles and objectives shape the network's primary function and limit secondary functions. An undisciplined architecture will create higher security risk and cost while failing to reliably support the electrical transmission system. Power system networks are different than enterprise and carrier networks in regards to data, devices and actor functions utilizing the utility network. The primary function of the utility's power system network is to protect, control and supervise the electrical flow from generation to consumption. Ideally, failures, impairments or outages in the utility transmission ICT network should minimally impact the reliability or security of the electrical systems power flow.

Critical network security begins with proper network architectural paradigms and the network system management to monitor, control and enforce architectural principles. Undisciplined architectural paradigms lead to higher security cost with less security while even a disciplined architecture without network system management only provides the gate with no guard [4]. Network system data object development is intended to provide the metrics, granularity and visibility into network systems to enable confident, secure and reliable management of interdependent electrical and ICT systems.

Utility networks have been shaped and operated for decades on voice based time slots and serial links between devices, actors and services. Emerging utility networks are being built upon packet data networks which require a new discipline to leverage the benefits of intelligent devices and message delivery. New architecture principles and paradigms must emerge to serve the electrical elements' protection, automation and control objectives through ICT technologies with high security, reliability and system confidence within transmission bulk electric critical infrastructure. NSM's primary function is to identify and establish the appropriate data object models that can monitor, manage, and secure the ICT infrastructure of electrical automation networks.

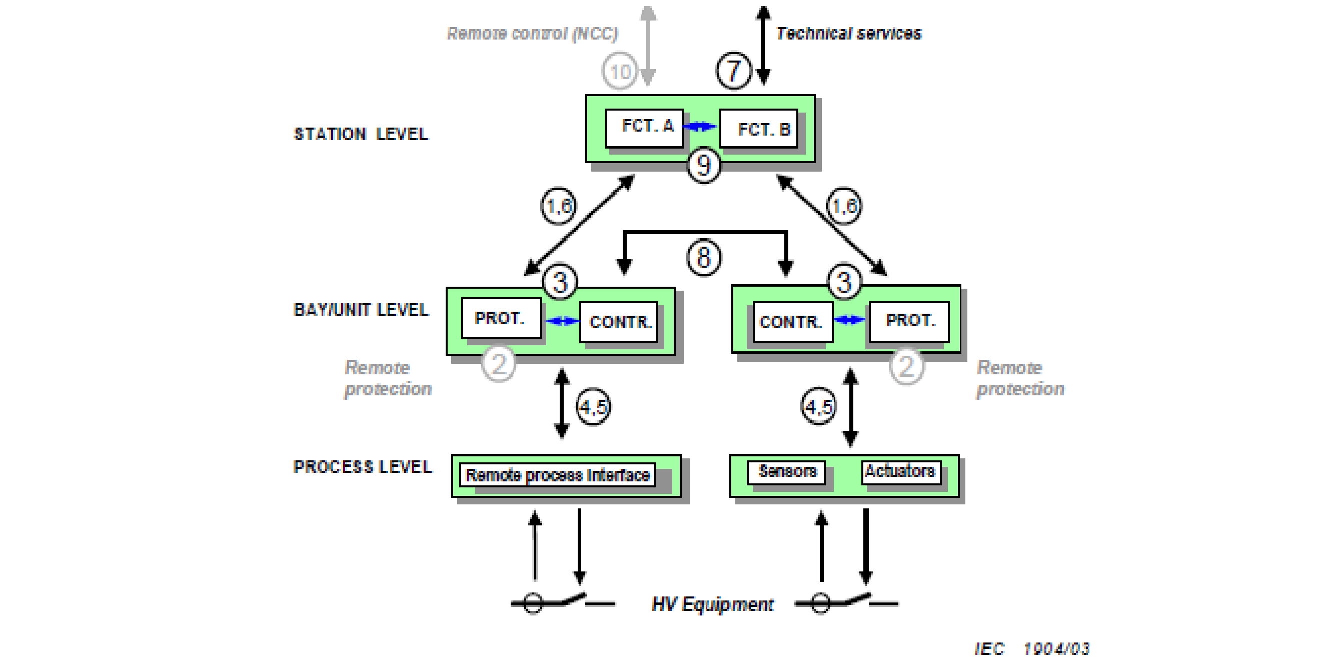
Although IEC 62351-7 applies to all areas of power system operations, this report starts with transmission substation automation. The following sections discuss Use Cases for three types of networks within substations:

- Substation Local Area Networks (SLAN) NSM Use Cases
- Substation-to-Substation Area Networks (SSAN) Use Cases
- Substation Wide Area Networks (SWAN) Use Cases

Substation Local Area Networks (SLAN) NSM Use Cases

Substation Monitoring and Control Configurations

Figure 3-1, from IEC 61850-5 [5], shows the typical Substation LAN (SLAN) configuration of operational data interchanges and identifies the functional Local Area Network levels utilized in substation designs. A transmission substation would commonly have an A and a B network to eliminate single points of failure.



IF1: protection-data exchange between bay and station level (***Substation LAN***)

IF2: protection-data exchange between bay level and remote protection (***Substation-to-Substation WAN***)

IF3: data exchange within bay level (***Process Bus***)

IF4: CT and VT instantaneous data exchange (especially samples) between process and bay level (***Process Bus***)

IF5: control-data exchange between process and bay level (***Process Bus***)

IF6: control-data exchange between bay and station level (***Substation LAN***)

IF7: data exchange between substation (level) and a remote engineer's workplace (***Utility WAN***)

IF8: direct data exchange between the bays especially for fast functions such as interlocking (***Process Bus***)

IF9: data exchange within station level (***Substation LAN***)

IF10: control-data exchange between substation (devices) and a remote control center (***Utility WAN***)

Figure 3-1
Station Interface

Additionally, the SLAN would have communication services and LAN connectivity for a station HMI interface, Disturbance Fault Recorders, ICCP and other actor services using a common Substation Station Gateway through IF7 and IF10. Substation Automation and protection in the SLAN is typically sub-cycle (<16.67mS) and technologies traditionally are RS485 ring networks. However, these are being replaced with packet technologies such as High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) which can offer transparent network recovery times.

Utility SLAN ICT can include:

- A Utility SCADA WAN Gateway/RTU between the substation and the utility control center
- Microwave

- Fiber Optic
- Power Line Carrier
- Radio Modems
- Leased Lines –traditionally for voiced based services
- Protection Communication Channel(s) between relays in different substations SSAN
- Direct Fiber
- Multiplexed xDS0 C37.94 Channels (SONET-Microwave and Fiber)
- Power Line Carrier, Tone and Pilot
- A Packet Substation LAN A and LAN B for most exchanges of data within a substation
- A Legacy Substation A and B Serial Rings with a Communications Processor/RTU
- A Process Bus LAN Packet or Serial Ring for very high speed interactions

Substation LAN: Copper Contact vs. Networked Sensors and Actuators

Cost savings in labor and materials to network yard sensors and actuator controls through process bus merging units are motivating factors in migrating to new technologies and protocols. However, the engineers' psychological confidence level in a hard contact versus a soft-state value provided by a multiplexed optical channel is a valid concern and needs to be addressed. It is clear that the information infrastructure must be managed to the same level of reliability as is provided for power system reliability.

NSM objects focused on the merging unit(s) local area network service between the process and bay nodes within a 61850 transmission substation would provide a system method for increasing engineering confidence in networked actuators and sensors. The advantages of being able to directly multiplex multiple sensors and actuators through an optical process bus merging unit while maintaining high reliability visibility allows a reduction in hard contact copper consumption and increases engineering confidence in soft-state reporting. Space-confined transmission substations also benefit by a reduction in the trenching requirements for hard contact cabling through networked sensors, breakers, switchgear and actuators where NSM provides the object monitoring and security of process bus links (IF4 and IF5 from figure 2) from merging units or cabinets to the bay level. IEC 62351-7 management of objects in the process bus to bay bus interface could increase operational visibility of networked systems, yard port security and engineering confidence.

Substation LAN: End Device User Connectivity and Security

Intelligent Electronic Devices (IEDs) or End Devices embedded with NSM objects would be of value to operations. NSM could provide the control operator with the ability to test a given sensor, actuator, relay or network element's port by performing a remote loop back and embedded test pattern generation test function to verify the health and performance of the communication channel.

The end devices in this power system monitoring process may include:

- Substation instrumentation, control and protection equipment (PT and CT sensors, breakers, protective relays, LTCs, capacitor banks, static var compensators, phase shifters, PMUs, digital fault recorders, fault locators, condition monitoring sensors, etc.)
- Substation SCADA Remote Terminal Unit (RTU) or Gateway that transmits the data from the substation systems on to the network.
- Power supplies and other auxiliary equipment
- SCADA system in the Control Center

Substation LAN: ICT Exchange Traffic Segmentation and Security

The NSM applications within the transmission SLAN could be utilized to monitor, manage and configure traffic segmentation, security, authentication, and access from the transmission exchange gateway to the SSAN and remote control centers.

Transmission substations have direct connectivity to distribution substations which can often be located within the same station real estate. DER also directly connects to transmission substations and shares line protection. DER may also share network synchronization or other network resources where NSM could enable expanded secure access to 3rd party actors.

NSM Use Cases for Substation ICT Monitoring and Control

Setup and Maintenance of Substation LAN Devices and Network Elements

Monitoring and control of transmission substations through SCADA systems has been implemented by most utilities for several decades. This has often included some basic monitoring of communication networks and the health of some equipment, but generally uses proprietary methods with minimal remote control capabilities. These methods are not interoperable across different vendor equipment and systems. By applying IEC 62351-7 and NMS, it is possible to provide monitoring, maintenance and security of communication channels, devices and ports. Benefits from extending this are shown through the following use cases. The Use Cases in Table 3-1 describe the initial set up and on-going monitoring and maintenance of transmission substation communication networks and end device configurations.

Table 3-1
Use Cases: Substation Setup and Maintenance

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
1	Determine connectivity of primary Substation LAN equipment	Report primary connectivity status	• NSM application • Communication nodes on Substation LAN • End devices on Substation LAN	• Utility WAN • Substation LAN	• Maintenance function • No timing constraints • May impose heavy traffic; implementation dependent
2	Determine connectivity of backup Substation LAN	Report secondary connectivity status	• NSM application • Communication nodes on Substation LAN • End devices on Substation LAN	• Utility WAN • Substation LAN	• Maintenance function • No timing constraints • May impose heavy traffic
3	Test Substation LAN recovery and protection times	(In maintenance mode), test link, ring and node primary to secondary switching times and recovery	• NSM application • Communication nodes on Substation LAN • End devices on Substation LAN	• Utility WAN • Substation LAN	• Maintenance function • No timing constraints • May impose heavy traffic
4	Monitor changes to access control list (ACL)	Monitor changes to the ACL in the Substation Master/firewall	• NSM application • Substation Master and/or firewall	• Utility WAN • Substation LAN	• Monitoring function • No timing constraints
5	Determine security configurations	Verify security and access control settings of applications in devices on the Substation LAN	• NSM application • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Monitoring and maintenance function • No timing constraints
6	Determine traffic priority configurations	Verify QoS, CoS, CBIR and queue weighting and class parameters for critical traffic	• Intranet operations network • Extranet 3rd party configuration priority symmetry	• Utility SWAN • Substation gateway	• Network engineering function • Monitoring function flag conflicts • Maintenance function

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
7	Test connections to end devices	Verify that all authenticated access to end devices are possible	• NSM application • End devices on Substation LAN	• Utility WAN • Substation LAN	• Maintenance function • No timing constraints
8	Test end device responses to losses of connectivity	Determine that end devices take appropriate action on loss of primary or backup connections, including reversion to local control	• NSM application • End devices on Substation LAN	• Utility WAN • Substation LAN	• No timing constraints
9	Control connections	Modify the configuration of the Substation LAN Disable ports, devices or channels	• NSM application • End devices on Substation LAN	• Utility WAN • Substation LAN	• Security and maintenance function • No timing constraints
10	VLAN configuration	Ensure VLAN configuration is inline with power system domain requirements	• NSM application • Substation engineering workstation • Network elements	• Substation LAN	• No timing constraints

NSM Use Cases during Operations

The Use Cases in Table 3-2 describe NSM during operations, which includes receiving alarms, issuing autonomous commands where these are established, recommending commands for operators, collecting statistics, and collecting NSM alarm and event logs.

Table 3-2
Use Cases: Substation Operations

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
1	Monitor communication nodes	Receive alarms and events on the status of communication nodes	• NSM application • Communication nodes on Substation LAN	• Utility WAN • Substation LAN	• Alarms within 1 second • Statistics sent periodically or upon request
2	Monitor routing algorithms	Trigger alarms when traffic path weighting changes traffic flow	• Utility intranet • Management and control plan monitoring • Critical traffic monitoring protection and automation time sensitive functions	• Utility WAN	• Identify and flag traffic pattern trend changes • Identify "path wander"
3	Monitor end device health	Receive alarms and events on the status of end devices, including "keep-alive" heartbeats, resets, restarts, etc.	• NSM application • End devices on Substation LAN	• Utility WAN • Substation LAN	• Alarms within 1 second • Statistics sent periodically or upon request
4	Monitor application health within end devices	Receive alarms and events on the status of applications within end devices, including any aborts, restarts, hanging, etc.	• NSM application • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Alarms within 1 second • Statistics sent periodically or upon request
5	Manage temporary and permanent communication failures	Receive alarms on communication failures and degradation of throughput, monitor responses to failures (e.g. backup, reconfiguration, etc.), collect statistics, and maintain logs	• NSM application • Communication nodes on Substation LAN • WAN Communication Nodes and Channels	• Utility WAN • Substation LAN	• Alarms within 1 second • Statistics sent periodically or upon request

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
6	Monitor communication protocols for errors	Receive alarms on communication protocol errors, including version mismatches, malformed packets, time synch errors, etc.	• NSM application • End devices on Substation LAN	• Utility WAN • Substation LAN	• Alarms within 1 second • Statistics sent periodically or upon request
7	Monitor data errors	Receive alarms on data errors, including invalid data detected, invalid control commands, data access errors, missing data, etc.	• NSM application • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Alarms within 1 second • Statistics sent periodically or upon request
8	Control applications in end devices	Control applications through start, restart, kill, switch to backup end devices, etc.	• NSM application • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Control commands sent within 1 second
9	DER communications	Ensure communication segment status and security to enable the use of DER for power operations	• NSM application • DER communication equipment • Time sync monitoring	• Substation LAN extranet and internet actor communication links • Synchronization networks	• Monitor link times and hop counts within mS • Ensure channel segmentation security

NSM Use Cases for Cyber Security attacks

Cyber Security attacks can affect the communications infrastructure, thus compromising the power system management. Table 3-3 describes scenarios where NSM would improve cyber security monitoring and management.

Table 3-3
Use Cases: Cyber Security Attacks

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
1	Cyber security management	Monitor end device access and connectivity	• NSM application • End devices on Substation LAN • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Actions within 1 second
2	Intrusion detection and prevention	Detect abnormal number of login failures, resource exhaustion, unauthorized connection attempts, excess idle time, and other denial of service attacks	• NSM application • End devices on Substation LAN • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Actions within 1 second
3	Detection of coordinated attacks	Correlate failures across multiple substations, including time synchronization	• NSM application • End devices on Substation LAN • Applications in end devices on Substation LAN	• Utility WAN • Substation LAN	• Actions within 1 second

Substation-to-Substation Area Networks (SSAN) Use Cases

Substation to Substation

Substation to substation area networking (SSAN) will be an area of great transformation for transmission operation over the coming decades. As more complex automation of electrical networked sources emerge along with a continual need to optimize transmission lines and facilities, ICT will become critical to enabling a diverse set of generation sources and managing the changing complexity of the distribution load. HVDC, Flexible AC Transmission Systems (FACTS) and integrating bulk renewable generation sources are all changing the transmission landscape. ICT is playing a central role in the information exchange that advances and enables the rapid dynamic response, stable variable output and reliable power flow delivery of the transmission exchange station. NSM's role in this transformation is managing, securing and maintaining the ICT networks to enable the transmission exchange in electrical ring mesh networks.

SSAN will evolve from protective relaying, remedial action schemes (RAS) or special protection schemes (SPS) to leverage the value of electrical node distributed intelligence. SSAN NSM use cases may focus on advancing the substation-to-substation automation capabilities with new broadcast and multicast messaging capabilities in new protocols based upon packet-network technologies. NSM would add value in verifying the physical and logical integrity of the ICT channels serving real-time automation applications within synchronized meshed electrical networks. This would improve automated networking between transmission exchanges and reducing the burden on control center operations.

The SSAN communicates measurement, command and status variables between stations (IF2) or remote control centers (IF10) which were originally out of IEC 61850 scope. However, ongoing interest and work with synchrophasors and packet enabled measurement multicasting between substations encourages more development in protocol and network activity between substations. The concern of cascading outages caused by events that exceed the operational and automated protect scheme capabilities could find remediation through cooperative substation networking. Developing IEC 62351-7 NSM objects and functionality to improve awareness and confidence in regional instrumentation, control and protection messaging through networked intelligent stations would be beneficial in advancing wide area situational awareness and more reliable automation and protection across large regional areas served by transmission substations. NSM working with operational protocols could provide the network messaging time information to operational protocols, enhancing the time-domain performance of RAS/SPS or other regional schemes. The improved awareness and cooperation between the electrical system and its network elements could reduce unnecessary load shedding, maximize existing capacity and enhance system reliability for substation to substation automation operations.

Protective Relaying Configuration

Table 3-4 shows the classical SSAN demarcation between telecom/communication networks and protective relaying. Location A represents a substation connected through a communication network to Location B substation to provide communication aided protection. Utility telecom network engineers are responsible for providing a communication channel that meets BES reliability and security requirements to the line of demarcation. Protection engineers are then responsible for the relay and breaker operations and functions. IEC 62351-7 objects would allow management, monitoring, security and performance visibility of the teleprotection channel by monitoring port activity and channel performance.

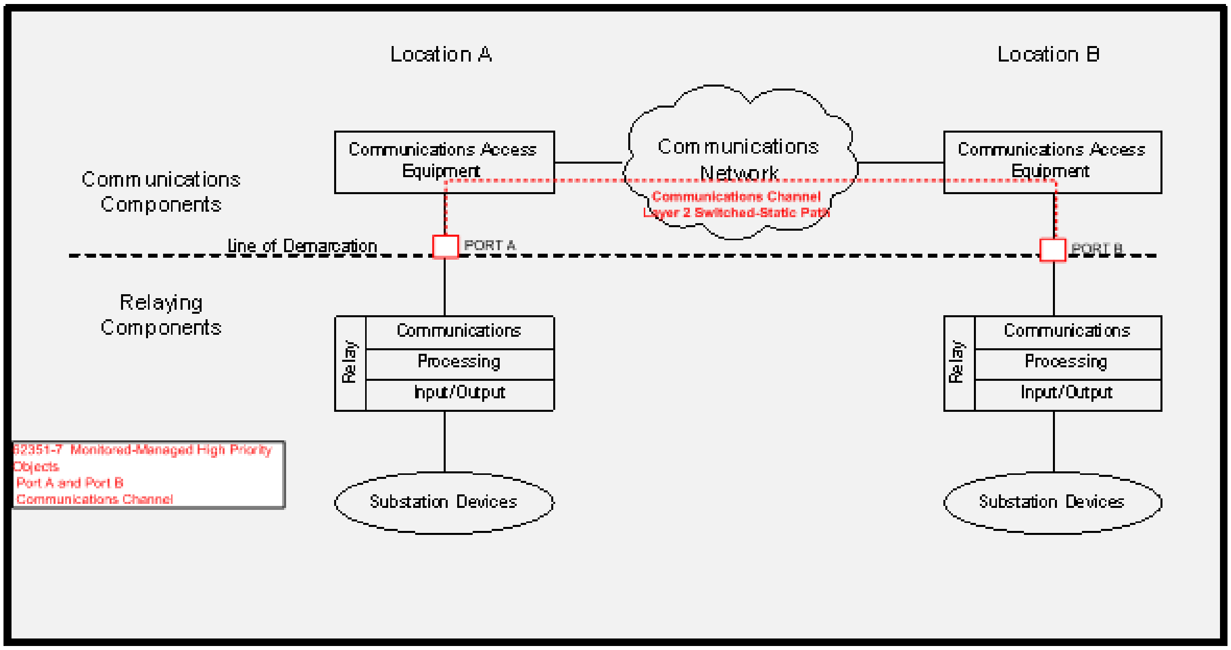


Figure 3-2
ICT and Protection Demarcation

Protective Relaying Functions

Protective relaying is used to trip the appropriate substation breakers in cases of power system events, such as over-voltage, under-frequency, distance relaying events, etc. An engineer sets the protective relaying coordination criteria for tripping and not-tripping with the objective of quickly removing the faulted elements and minimizing the number of elements taken out of service. Telecommunications or network connectivity is utilized to enhance the speed of relaying operation and minimize the number of elements taken out of service by passing the appropriate messages between remote zones. Protective schemes and functions chosen by the protective relaying engineer determine the critical nature of the communication links. Protective relaying channel performance times are also determined by the application. Line protection applications typically have the longest times due to media signal propagation while the electrical bus applications residing within the Substation LAN have the shortest message times. The protective relays continually monitor the power system (voltage, current, frequency) and each other to coordinate actions through wide area communications channels or locally depending on the protected element and scheme. Channel performance, determinism and reliability (dependability and security) are critical since the communication channel should not impair or reduce the protected elements availability. Differential current protection scheme is one application which relies on a communication channel for the measurement values which ingress and egress a protection zone to discern a faulted state. Channels serving a differential scheme across physically redundant primary and secondary paths must have deterministic performance to avoid impairments to the dependability and security of the protection system.

NSM Use Cases for Protective Relaying

The following table identifies the main Use Cases associated with protective relaying with a focus on the communication network and system equipment, rather than the actual power system functions. These Use Cases cover performance issues and identify cyber-security requirements.

Table 3-4
Use Cases: Protective Relaying

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
1	Determine connectivity of primary Process Bus equipment	Request all nodes (communication nodes and end devices) to report connectivity status	• NSM application • Communication nodes on Process Bus • End devices on Process Bus	• Substation LAN • Process Bus LAN	• Alarms within 1 second • Statistics sent periodically or upon request
2	Inform network time settings for protective relaying	Inform engineer of protective relay channel settings	• NSM application • Engineer • Engineering system • Protective relays	• Utility WAN • Substation LAN • Process Bus LAN	• Link latencies • Priority monitoring • A and B symmetry
3	Monitor path latency, symmetry for primary, secondary and emergency channels.	Path changes may affect engineering parameters like "hold" times and other time sensitive protective parameters. Control and Engineering would be alerted and actual network configuration noted. During an event reconstruction, the network's state which may affect time correlation should be analyzed for the pre, during and post event	• NSM application • Protective devices • Telecommunicat ions engineer • Protection engineering	• Utility WAN	• Active Synchronization monitoring • Path latency changes reported within current capabilities.
4	Monitoring health/security of protective relaying channels	Substation Gateway monitors health and security of protective relay channels	• NSM application • Substation gateways • Protective relays • Breakers	• Substation LAN • Substation-Substation Area Network • Utility WAN	• Currently mS , future timing constraints will be uS

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
5	Network performance assurance	Monitor the performance of message delivery to ensure all system functions can be continually supported by the network	• NSM application • Network elements • Protective relaying devices	• Substation LAN • Merger Cabinet Process Bus LAN • Substation-Substation Area Network • Utility WAN	• mSec • Bit error rate (BER)

Substation Wide Area Networks (SWAN) Use Cases

Substation Wide Area Networks (SWAN) include at minimum a single control center where electrical and network activities are supervised, controlled and recorded. SWANs often, however, provide network connectivity to multiple control centers such as balancing authorities and Independent Service Organizations (ISO) which consist of intra, inter and extra-net domain connectivity of electrical grid operations information and data sets. SWANs support, control and supervise RAS/SPS, load balancing and stability of an interconnected grid.

WAMPAC Functions

Phasor measurement units (PMUs) capture streaming, sub-cycle data from sensors that are connected to the power system as Sample Value streams. This PMU data can be used to detect abnormal waveform shapes (power quality) and phase differences across very large areas that are synchronized to the same frequency, such as the Eastern Interconnect, the Western Interconnect, and ERCOT in Texas. Information collected can be analyzed to reveal possible power system problems across a large regionally interconnected grid. Local substation devices can also capture critical status and measurement data cycles that support this analysis in stored histograms. Control commands, either automated such as protective relaying or manual such as operator commands, can then be issued to mitigate these possible problems through load balancing or other actions.

WAMPAC Configurations

PMUs and the other equipment used for WAMPAC are located primarily in transmission substations (although distribution and other non-substation sites are also being utilized in some cases). The sensors are monitored and time-stamped continuously by the PMUs, and that data is sent to collectors where it is then transmitted to many control centers throughout the territory as shown in the figure below. The accuracy of the timestamps is critical in order to synchronize all of the PMU data.

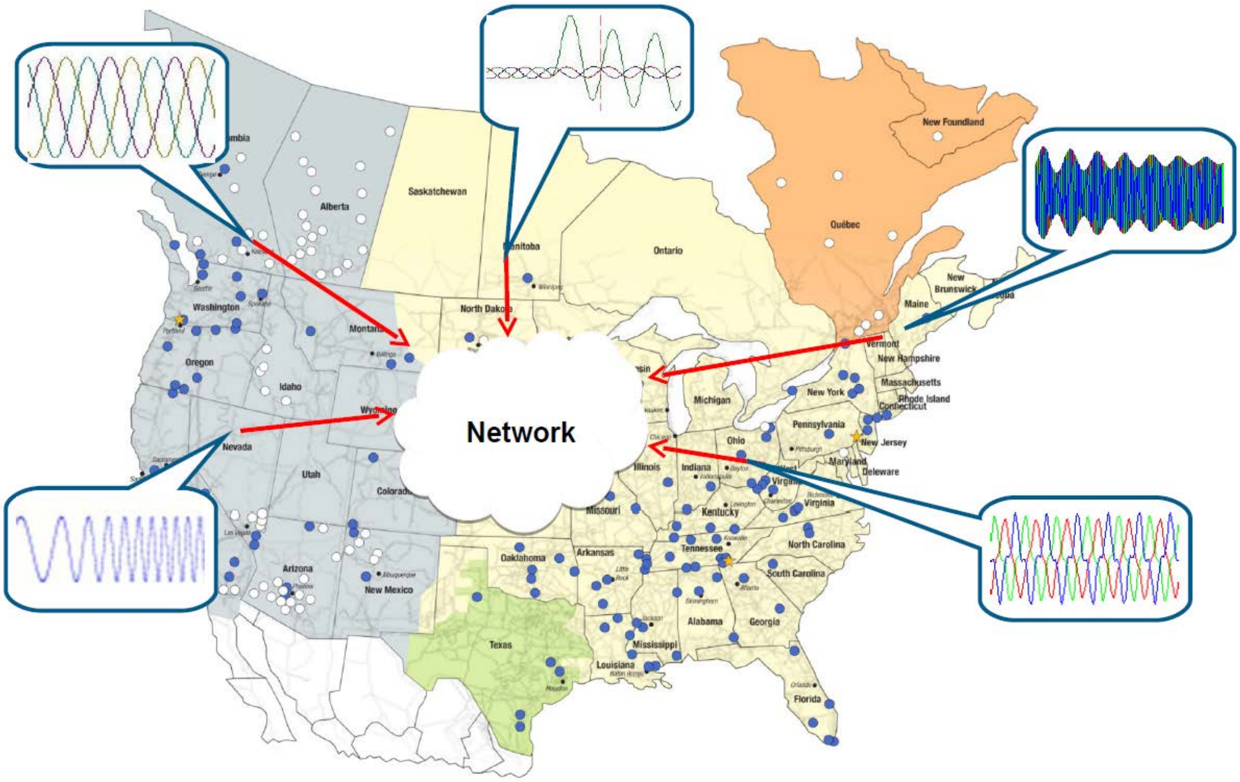


Figure 3-3
Regional SWAN Centralized Supervision and Control

NSM Use Cases for WAMPAC

The Use Cases in Table 3-5 describe scenarios where the WAMPAC function could be enhanced by NSM.

Table 3-5
Use Cases: WAMPAC

#	Use Case Name	Use Case Functions	Actors	Communications	Performance
1	Network configuration change management	Traceability for all changes to network element configuration	• NSM application • Engineering system • Network elements	• Utility WAN from engineering station to substation • Substation LAN	• Engineering functions • No timing concerns
2	Reporting real-time network transit times, latencies and packet performance	Allowing network times and performance visibility to wide area multiple domain networks	• NSM application • All recipients and users of PMU data. • Reports network time skew between different synchronized users	• Utility WAN • Utility to Utility WAN • Utility to ISO/Balancing Authorities/Reliabilit y Coordinators • ACE	• Monitoring function
3	Identify Traffic Congestion and Message loss	Provide cleansed actor data on network issues impacting message delivery	• NSM application • External actors of PMU data collection • Utility network	• Utility WAN • Utility to Utility WAN • Utility to ISO / Balancing Authorities / Reliability Coordinators • ACE	• Monitoring and reporting function
4	Monitor clock synchronization	Monitor and compare all clocks being utilized within a given system	• NSM application • GPS receiver equipment	• GPS Satellite signals to GPS receiver • Process bus from GPS receiver to PMUs	• 100 ms time latency • 50 µs max timing error
5	Monitor peripheral sensors	Monitor the availability of substation sensors being used by PMU's	• NSM application • Sensors • Multiple PMUs	• Substation LAN Process bus • Utility WAN	• Report by exception • SCADA polling times

4

SYSTEM EXAMPLE: SECURITY BREACH

A demonstration of Network and System Management was implemented which characterized a physical breach of an electrical substation followed by a network breach.

Demonstration Example: Substation Intrusion Detection Scenario

1. Assume physical breach of the substation; then access to a switch yard control cabinet

2. IED is disconnected from the network, and rogue device connected

3. NSM detects the rogue device, sends notification, and takes action to disable communications port (if desired)

An electrical transmission substation with a centralized SCADA control and private utility WAN forms the baseline scenario. Within the substation, an RTU connects to devices supporting serial communications such as a transformer monitor, as shown in Figure 4-1.

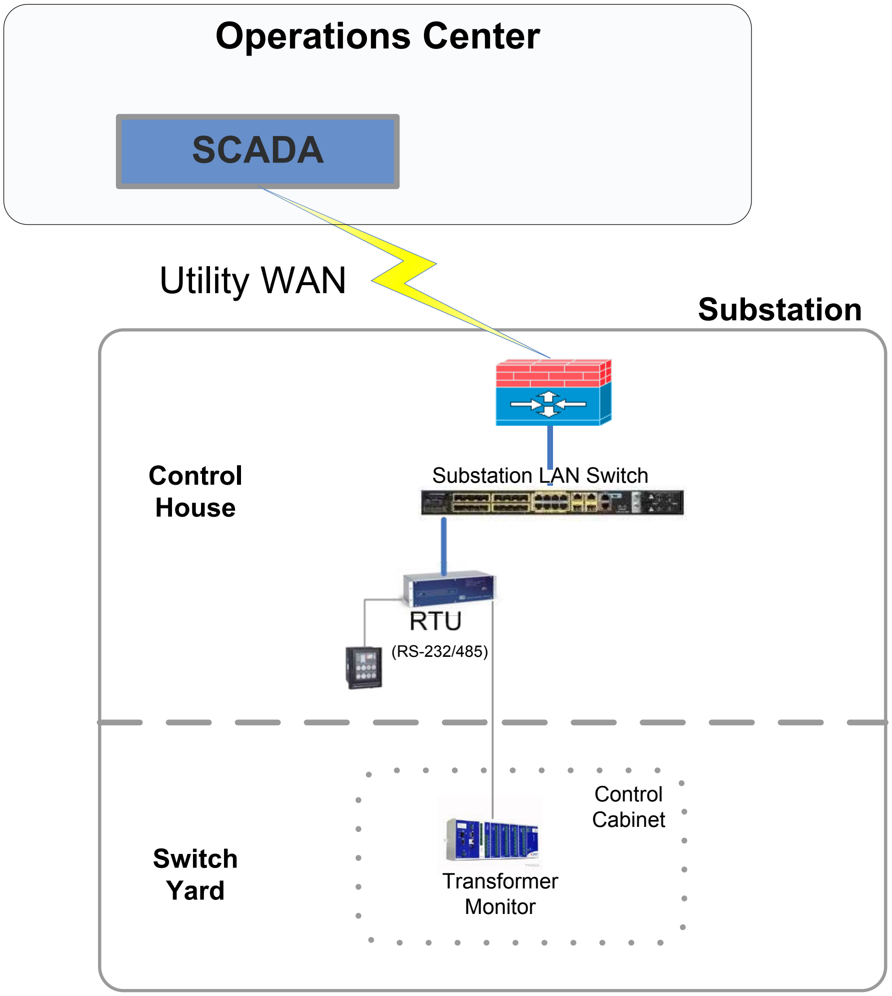


Figure 4-1
Substation Control Baseline

As with many systems, this substation’s network is evolving with more connected devices using Ethernet and Internet Protocol (IP). The next generation of the transformer monitor then supports IP and is connected to the substation LAN directly from the switch yard control cabinet, as shown in Figure 4-2.

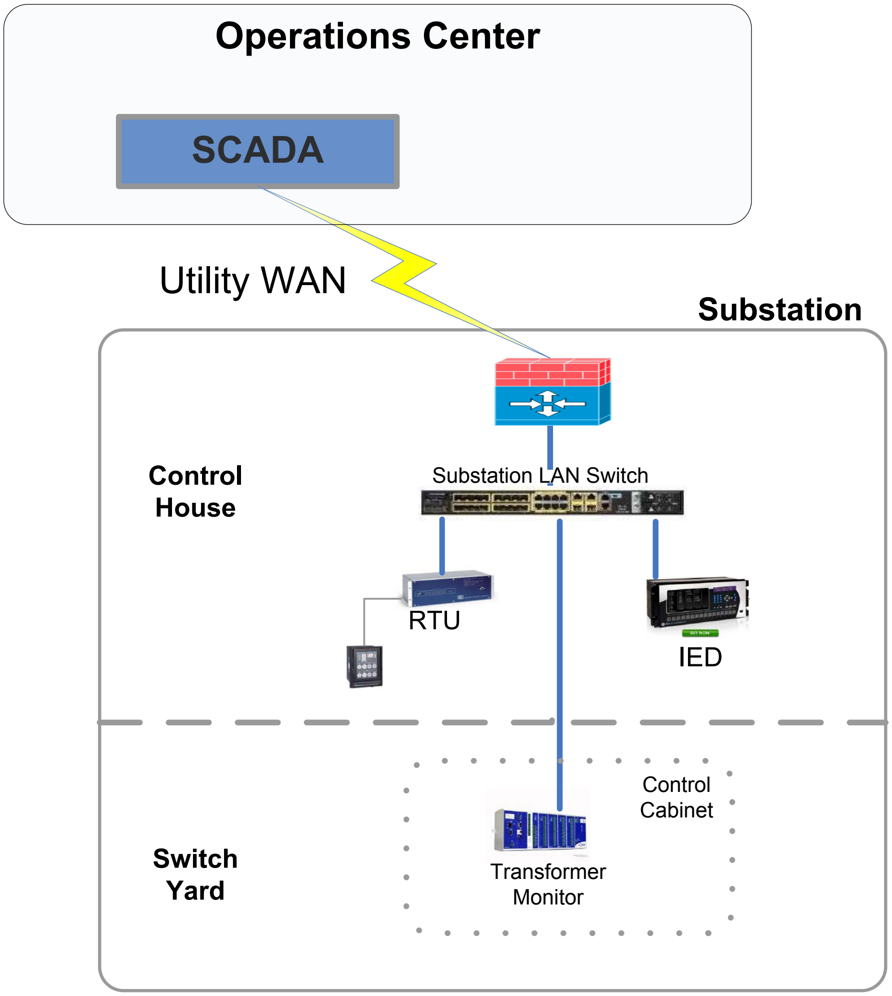
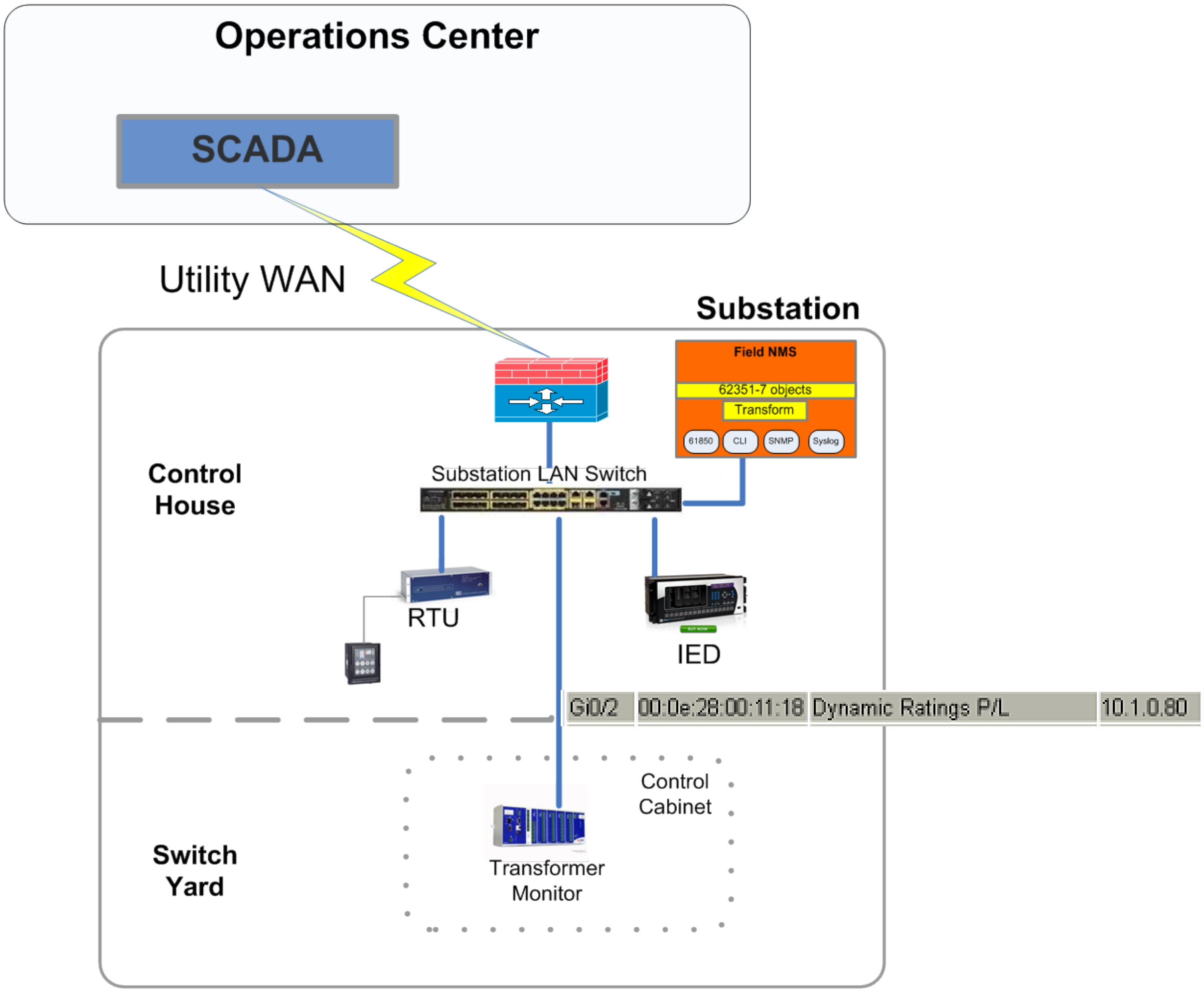


Figure 4-2
Expanding Use of Intelligent Devices and IP

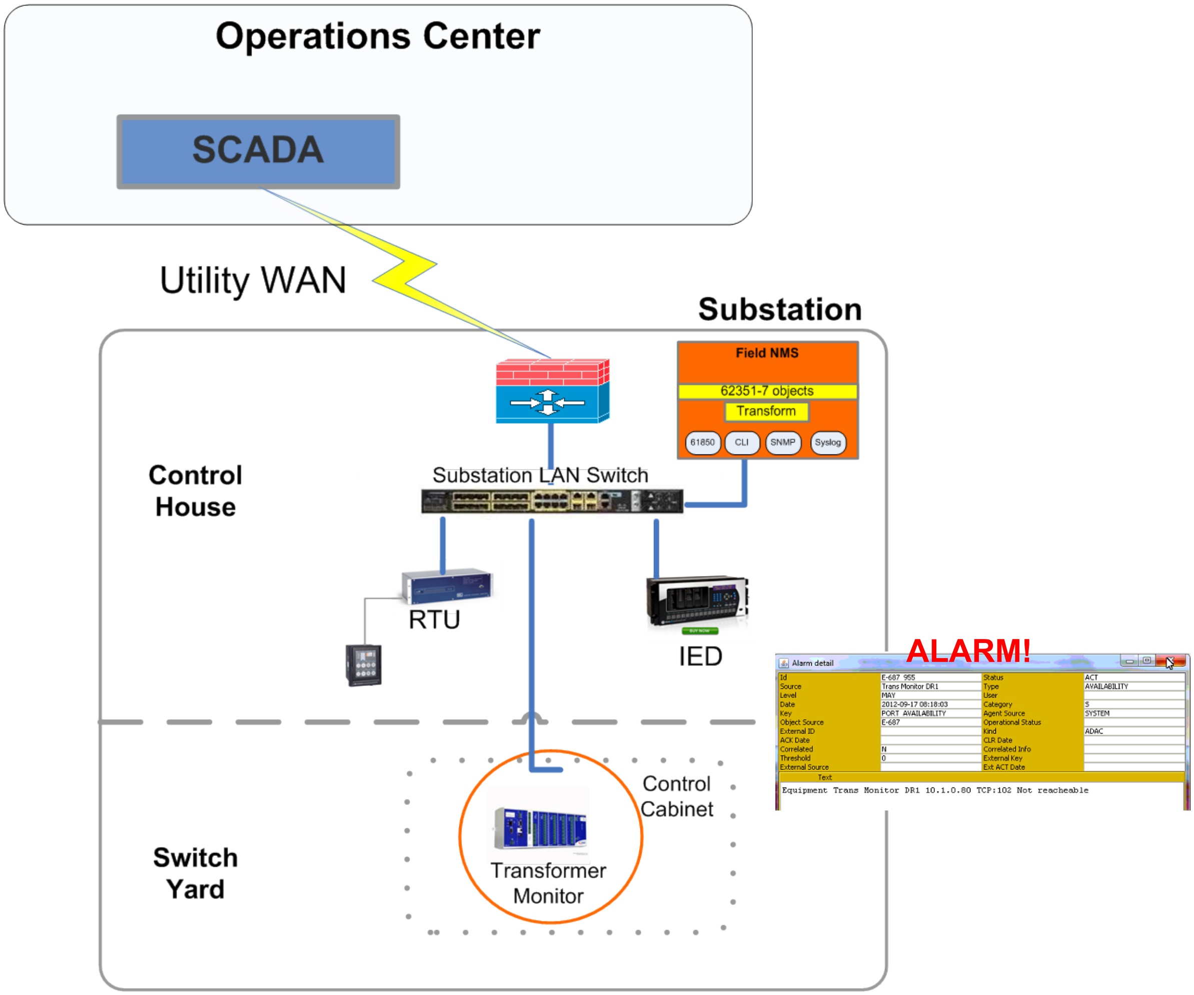
In order to ensure the reliability and security of the substation LAN, a Network and System Manager is deployed within the substation. This runs on a single server (or virtual machine) located in the control house as shown in Figure 4-3. The NSM understands and monitors many aspects of the communications systems and connected devices. For example, the system has identified the connection of the transformer monitor on port 2 of the switch, including MAC and IP addresses.



Gi0/2	00:0e:28:00:11:18	Dynamic Ratings P/L	10.1.0.80

Figure 4-3
The Addition of a Network and System Manager

A physical breach of the switch yard control cabinet results in the loss of connectivity of the transformer monitor, with alarm notification provided from the NSM. The network disconnect and alarm notification are shown below in Figure 4-4.



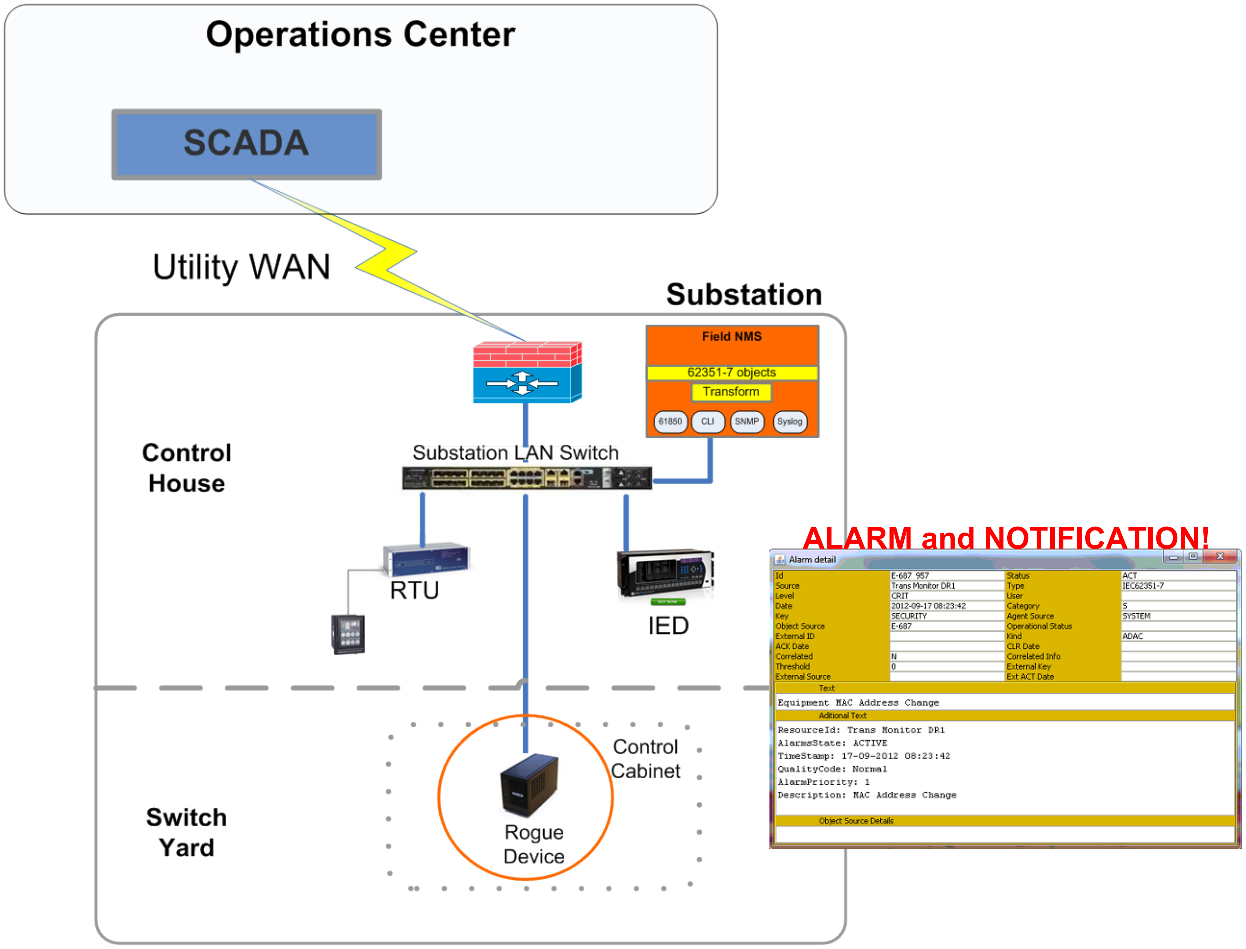
Id	E-687 955	Status	ACT
Source	Trans Monitor DR1	Type	AVAILABILITY
Level	MAY	User	
Date	2012-09-17 08:18:03	Category	S
Key	PORT AVAILABILITY	Agent Source	SYSTEM
Object Source	E-687	Operational Status	
External ID		Kind	ADAC
ACK Date		CLR Date	
Correlated	N	Correlated Info	
Threshold	0	External Key	
External Source		Ext ACT Date	

Text

```
Equipment Trans Monitor DR1 10.1.0.80 TCP:102 Not reacheable
```

Figure 4-4
Physical Breach and Disconnect

A rogue device is then attached to the network, with the same IP and different MAC ID as the transformer monitor. Upon reconnection, the NSM contains rules to check the device per the policies setup for the substation management. In this case, the presence of a different MAC ID causes a critical security alarm. Additional rules and device interrogation can be carried out as required to ensure complete trust. This is shown Figure 4-5 below.



Id	E-687 957	Status	ACT
Source	Trans Monitor DR1	Type	IEC62351-7
Level	CRIT	User	
Date	2012-09-17 08:23:42	Category	S
Key	SECURITY	Agent Source	SYSTEM
Object Source	E-687	Operational Status	
External ID		Kind	ADAC
ACK Date		CLR Date	
Correlated	N	Correlated Info	
Threshold	0	External Key	
External Source		Ext ACT Date	

Text

```
Equipment MAC Address Change
```

Aditional Text

```
ResourceId: Trans Monitor DR1
AlarmsState: ACTIVE
TimeStamp: 17-09-2012 08:23:42
QualityCode: Normal
AlarmPriority: 1
Description: MAC Address Change
```

Object Source Details

Figure 4-5
Rogue Device Detected

The above example of intrusion detection illustrates end-to-end monitoring and security policy enforcement use case.

Implementation using IEC 62351-7 Objects

IEC 62351-7 provides an abstract data model for information security objects. At this point, the standard provides an outline of requirements and potential objects, with some indication of potential implementation. The concept of Network and System Management involves native objects within devices, as well as calculated objects correlated from device and network status. Device level implementation will require the assignment of specific protocols to specific objects, assuring a convention which will enable interoperable implementations by multiple parties or vendors.

During the course of this study, no known devices have implemented these objects. A structure for implementing IEC 62351-7 information security objects was created within the NMS system using existing protocol adapters and a transformation layer to convert from the device native objects to this new model. Figure 4-6 shows these layers and available native protocols.

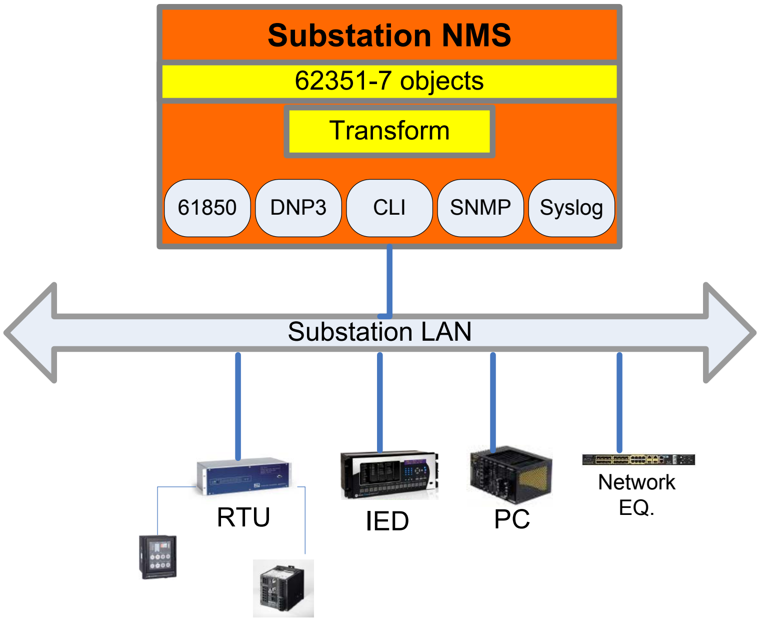


Figure 4-6
Transformation Layer for IED 62351-7

For the demonstration scenario, a parallel analysis model was created using 62351-7 derived objects. Device status was acquired from 61850 and SNMP protocol adapters from the IED and switch devices respectively. Rules were executed to achieve the results, just as were determined in the proprietary modeled trial in the previous section. The objects and values were represented in a GUI page showing the status dynamically.

While this trial was technically successful, the implementation was open to significant interpretation as described in the appendices. Several assumptions were required to create a specific format for some object attributes. The 62351-7 standard is relevant now for its concepts and awareness to the importance of this management space. Future versions will identify exact protocols for each type of object/device combination. With this greater specificity and additional overall vetting, the standard will become useable for these situations.

5
RECOMMENDATIONS / NEXT STEPS

Network security begins with proper network architectural paradigms and a network system management to monitor control and enforce architectural principles. Undisciplined architectural paradigms lead to higher security cost with less security while even a disciplined architecture without network system management only provides the gate with no guard. Network system data objects are intended to provide the metrics, granularity and visibility into network systems to enable confident, secure and reliable management of interdependent electrical and ICT systems.

This project's objective is to begin development of a standard set of network system management objects for bulk electrical transmission systems to serve the network system management (NSM). NSM objects will provide increased visibility on network system performance, security and control of the management of critical infrastructure networks. The resulting benefits include better situational awareness and improving critical infrastructure security, which ultimately leads to better reliability directly benefiting automation, analytics and further advancement of intelligent grid initiatives serving the bulk electrical transmission systems.

This project stage developed a first iteration of a use case based approach for analyzing transmission system information infrastructure management. The next stage requires the formalization of this approach within a specific domain, which can then be duplicated and expanded to additional scenarios and domains.

Substation control networks are the anticipated focal point, with the main objective being to implement a subset of NSM functionality monitoring both network and power devices with a single system based upon an aligned set of data objects.

Recommendations for next steps

A conceptual model for future work is laid out below in Figure 5-1. This diagram targets an engagement focused on the priority use case scenarios, which are expanded upon to extrapolate technology agnostic requirements. An assessment of technologies can then lead to specific implementations.

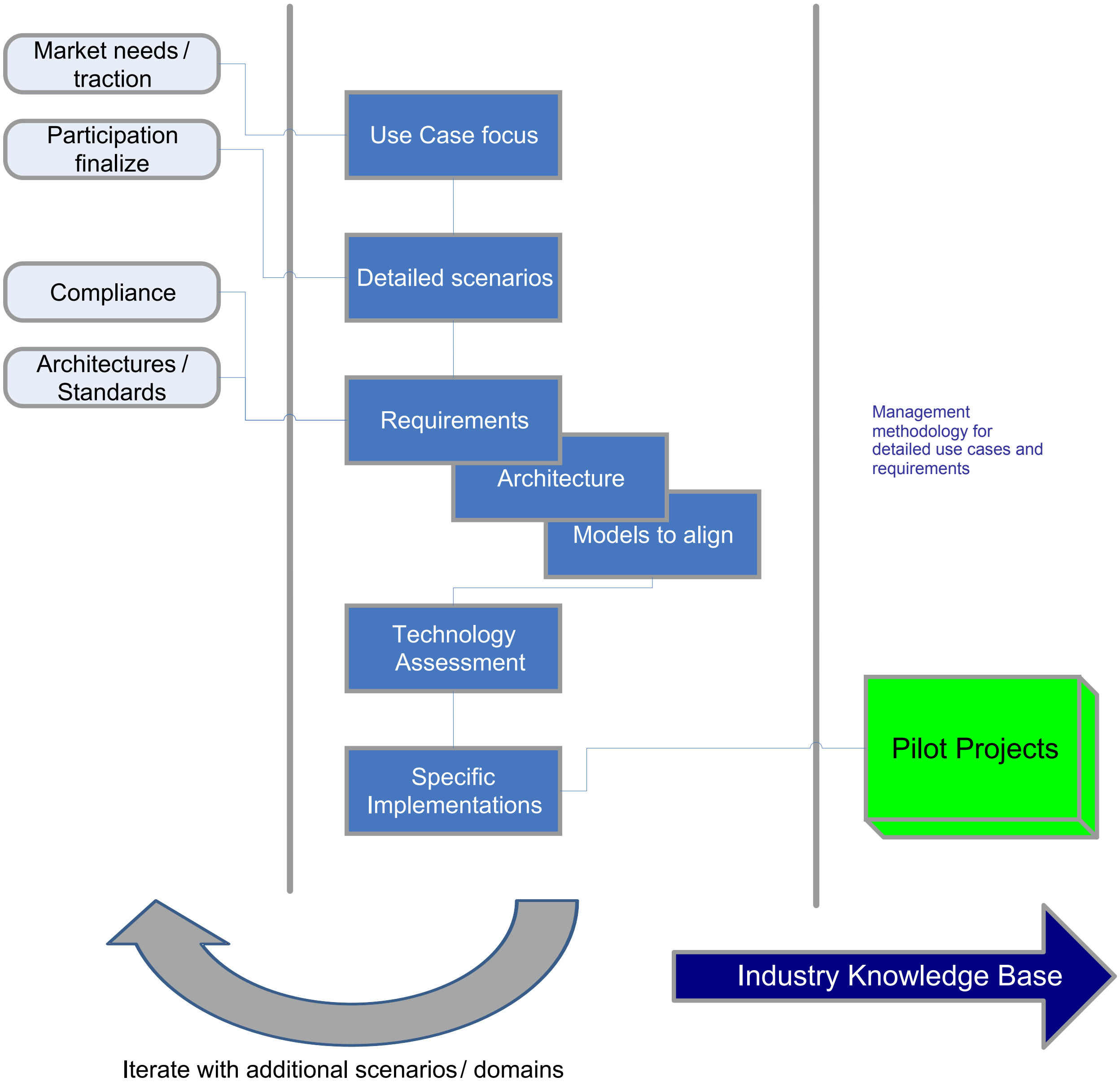


Figure 5-1
Conceptual model for future work

Recommended next steps

- Expand scenarios to include greater detail utilizing in an industry accepted format.
- Review IEC 62351-7 and expand it for both functional and non-functional objects which are technology agnostic.
- Develop requirements specific to particular architectures.
- Develop requirements specific to enterprise models such as CIM.

- Determine which protocols, devices and implementation methods are available for use with NSM.
- Examine the impact of specific implementations, which may include the extension of standard protocols, vendor engagement and lab trials, as well as specific NSM features.
- Engage with specific utilities to develop pilot projects that can extend their existing management systems and devices to include NSM functionality.
- Continue to develop an industry knowledge base for determining future requirements, lessons learned, best practices and feedback for IEC TC57 WG15.

A
REFERENCES

1. IEC 62351-7, *Network and system management (NSM) data object models*, Edition 1.0, 2010-07. [standard]
2. IEC 62351-1, *Power systems management and associated information exchange – Data and communications security, Part 1: Communication network and system security – Introduction to security issues*, First Edition, 2007-01. [standard]
3. IEC 62351-10, *Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines*, Edition 1.0, 2010-01. [standard]
4. T.R. Janca, "Utility Ethernet network architecture: Networked Electrical eXchange Topology-NEXT," presented at the 2012 35th IEEE Sarnoff Symposium, May 2012, Newark, NJ. [conference paper]
5. IEC 61850-5, "Communication networks and systems in substations – Part 5: Communication requirements for functions and device models," First Edition, 2007-01. [standard]

B

FEEDBACK: IEC62351-7 REQUIREMENTS

IEC62351-7 section 6 defines “Security and reliability NSM requirements for power system operations”. Developments in network security technology since its initial publication in July 2010, along with identified ambiguities in the standard’s language, provide an opportunity for document revision for the sake of clarity, consistency, and currency.

Below are observations and specific recommendations for revisions of section 6 and its subsections.

Table B-1
IEC62351-7 Section 6 Requirements Feedback

Section	Notes, Observations, and Recommendations
6.1.2	• Recommendation: replace "In addition to monitoring the network equipment, it is crucial to determine if the network can provide the performance it is designed for" with “Monitoring the status of network equipment also includes monitoring the status of communications links for traffic volume, latency in message delivery, degradation, failure, or other alteration in order to determine if it is providing the required performance." • Recommendation: Specify how to determine available bandwidth of (alternate) communications links: add “by periodically switching to these alternate links as part of a controlled testing process to validate the integrity of the alternate network configuration” • Recommendation: remove "detecting the status of backup or spare equipment for use in failovers" as duplicate of #1.
6.1.3	• Observation: Document seems to suggest a preference for using SNMP over 62351.7 objects where they exist. Clarification would be beneficial here. Recommend adding: “Where existing network management tools provide the required data and information, they should be used as an alternative to implementing separate network management objects.” • Recommendation: differentiate between “throughput” and “latency” and clarify how to measure throughput without impacting it. • Recommendation: change “lower than expected throughput” with “longer than expected latency” in all bullets in this section.
6.1.4	• Recommendation: clarify or remove the following statement: "However, some of the more detailed information must be collected by the protocol stacks, since that is where the knowledge of correct and incorrect protocol formation resides" given the prevalence of decoders for most mainstream SCADA protocols. • Observation: some of the bulleted items (see, e.g., "detecting mismatches of differing protocol versions and capabilities") do seem to imply detection at the endpoint. • Recommendation: change “detecting invalid application object access/operation” to “detecting invalid application object access/operation at network interfaces”. • Recommendation: deemphasize denial of service attacks using buffer overflows and generalize to the multiple impacts of buffer overflows,

	including privilege escalation and unauthorized access. • Observation: Physical access disruption would be detected by 6.1.3; this may be redundant in this section. • Recommendation: define "invalid network access" by adding “(e.g., unauthorized devices, unauthorized or inappropriate requests for network resources, and evidence of anomalous behavior)”
6.2.1	• Recommendation: add other security devices such as IDS and application firewalls to the following sentence, or remove the examples entirely: "External assessments must be performed by separate systems, such as gateways, proxy servers, and routers."; “External assessments must be performed by separate systems with the requisite security functionality, such as gateways, proxy servers, and routers.”
	• Observation: "anomalies in data access (e.g. individual request when normally reported periodically)" requires correlation that may not be possible on the endpoint. This therefore implies some sort of SIEM that can provide this capability.
6.2.2	• Recommendation: Clarify whether the requirement to "shut down another end system" really implies that end systems should be able to control other end systems. Change “The following is a list of security control and management commands:” to “The following is a list of security control and management commands required of a comprehensive security and network management system:”
	• Recommendation: remove all references to lists of revoked users. Best practices would be to maintain lists of authorized users, with all others not on that list being unauthorized. Refer to “revoked credentials” where appropriate.
6.3.1	• Recommendation: rewrite "identity of unauthorized user" as "information regarding the identify of unauthorized user" • See 6.2.2 recommendation regarding revoked users.
6.3.2	• Recommendation: Eliminate references to "passive IDS" and replace with “IDS”. • Recommendation: Remove text starting with “Typically, the passive IDS” and ending with “standardized NSM data objects” and replace with the following section introduction: To mitigate the impact of denial of service attacks against critical control systems that result in resource exhaustion on the end device, a system must be implemented to capture and analyze suspicious network traffic. This analysis may be done at several points within the network, but is typically implemented using intrusion detection systems regardless of location. Both network- and host-based intrusion detection functionality should be evaluated as part of the overall system security design. • Recommendation: specify the units by adding the following parenthetical text: "exceeding the maximum number of connections permitted (per device and per application) over the network"

	• Recommendation: replace “count of number of connections actually in place over the network” with “count of number of authorized connections in place over the network in order to establish a baseline of authorized activity against which actual activity can be measured” • Recommendation: clarify what "below low level battery power limits or too high rate of change." means by adding “of battery discharge”.
6.3.3	• Recommendation: replace the first paragraph with the following: System security design must include provisions for detecting network-based buffer overflow attacks that could impact end devices. Intrusion Detection Systems in conjunction with endpoint monitoring may play an important role in detecting this anomalous network traffic. • Recommendation: maintain consistent wording ("overruns" vs "under runs" vs "overflow/underflow")
6.3.4	• Recommendation: replace references to “passive IDS” with “IDS”
6.3.5	• Recommendation: replace the first sentence with “An attack that results in a resource being powered off, disconnected, or otherwise rendered inoperable represents a serious denial of service.”
6.3.6	• Recommendation: expand/clarify the statement that "[f]irewalls are designed to prevent invalid access to networks, particularly through the use of access control lists which permit only authorized IP addresses to pass through the firewall" given that they're designed to help prevent invalid access, but are only truly effective as one layer of a multi-layered approach to perimeter security. • Recommendation: Remove text starting with “However, IDSs…” and ending with “For example,” (starting the new sentence with “Any protocols…” • Recommendation: remove “passive” when referring to IDS.

C
FEEDBACK: IEC 62351-7 DATA OBJECTS

This section is the result of a review of the attributes found in section 8 of IEC 62351-7. While the focus is on section 8 and the management objects it contains, it also incorporates comments/review of other aspects of the 62351-7 specification. In particular, sections 6 and 7 to the extent those sections impact the interpretation of the attributes found in section 8.

This review is not an exhaustive examination of all aspects of 62351-7, nor of the companion IEC specifications that it is related to. The focus is on section 8 and the enumeration of management objects it contains. Objects found in section 8 were evaluated from the following perspectives:

1. Utility – did an object add to our understanding of the state of the network or the constitutive network elements?

2. Clarity – did the definition provided include sufficient detail so that a competent engineer would be able to implement the object with the information provided?

3. Practicality - while an element of information can be desirable in the abstract, a key metric used in the evaluation of these objects was: would engineers at different organizations be able to create multiple, vendor-independent, interoperable implementations? Practicality includes factors such as: an assessment of whether the object could be effectively mapped to different vendor products while retaining consistent semantics and cost/ease of implementation. The analysis included whether the resulting systems created by engineers developing the instrumentation in the managed elements and the engineers that were implementing the fault, configuration, performance, security and accounting software in the management systems would function well when deployed. “Function well” includes evaluating performance impact on the managed devices, network and management systems.

4. Completeness – In some places, suggestions for additional objects are made that would further reliable, secure operations. See also a section on Recommended Additions.

Evaluation Perspective

This evaluation was based on a network management systems perspective. That is, based on what industry has learned after many years experience in the telephony, data networking network services, application and systems management environments. While there are concerns about the general approach for the integration of network-based information into the utility environment indicated by 62351-7, and to some degree these concerns surface in the evaluation of the objects, this was not a full architectural review of the environment. Its focus was only on the objects defined in this specification.

IEC 62351-7 Section 8 Review

Section 8.1.1 begins with:
The model of the physical network configuration, including the locations, the physical connections, and logical interconnections of the different network devices, is out of scope of this standard. However, it is assumed that an appropriate network configuration model is available so that when a network device sends information, its location and role in the network can be understood.

This raises several general questions/concerns:

1. Understanding the network configuration and logical/physical interconnections can be important elements when attempting to understand not only if a network is functioning correctly, but also what the source of a malfunction may be, whether it is due to an intentional attack, malfunction, or the result of a configuration error, the most common reason networks and the services they carry fail.

2. One of the key areas that network equipment vendors differ from each other, even when implementing a standard such as BGP or Differentiated Services is in the detail of the configuration objects. This is why there are no 'abstract' configuration standards for these devices that have been widely adopted[2]. Understanding these detail differences for configuration objects and related control and monitoring objects are fundamental to understanding if the network element, and by extension the network is functioning correctly.

3. As a general rule, network devices do not send information except in limited cases[3]. They do not tend to include topology information (at least in the management plane).

The section (8) assumes a standard network configuration model that has never existed in a standard form for IP network communication management systems. Management software vendors create their own proprietary model(s) based on an analysis of data collected from the network and other information.

Section 8.1.1 Additional Object Specific Comments

The first list below is under the category of Configuration settings in the table, but most of them are not in any sense configuration elements that a network element would understand.

1. EndLst – This definition requires a bit more specificity. Does it include key elements of the power environments that may not be directly network accessible but which are 'fronted' by a controller of some type such as a PLC? For a management/security

[2] The IETFs' nearly decade long NETCONF (Network Configuration) activity notwithstanding.

[3] Syslog is an example, but usually large streams of information from network elements are not collected (at least by the NMS – Network Management System. Netflow is generally targeted at specific issues though the data from both Syslog and Netflow are helpful in a failure analysis.

system to work well, it is helpful to include the components that are under threat, which in this case may have to be proxied by network communications gear. It is usually the case that the proxy does have the facilities to communicate with the non-networked devices so that important changes in configuration, fault status, performance, access, etc can be reported to the management environment.

2. NodList –More specifics would be helpful. For example, the inclusion of bridges implies an understanding of layer 2 topology which is good, but not complete.

3. PthLst – Is this at the physical, data link, routing or other layers? How is this to be determined? If these attributes are to have wide spread use for multiple interoperable implementations, all the attributes in the document require fuller specification[4].

4. ACLLst – A great deal more specificity is needed for this. This is a list for what systems or which parts of the systems? Most ACLs are also evaluated in specific order; does this include the facility for this attribute to be conveyed[5]?

5. PthRouteLst - This is difficult in an IP environment as it tends to be protocol/layer specific. For example, path definitions vary by routing protocol type. In environments that use facilities like MPLS this is further complicated. Different routing protocols use different metrics to evaluate priorities – some are dynamic.

6. ActSet – This is almost universally a device/technology specific activity. To the extent it is not, it assumes a level of software automation in the management plane usually discouraged by operational personnel. Also missing from this definition is the idea of directionality. In many environments, there may be primary or secondary paths or asymmetric routes established for a number of reasons. Understanding all these details are key to knowing if the network is really under stress/attack.

After reviewing this section, it appears that an additional column for each of the objects that describes the purpose/objective of the attribute would be helpful. Guidance about how they are to be created would also be beneficial.

[4] One of the hallmarks of a standard moving up the 'standards track' in the IETF is the availability of multiple interoperable implementations. Absent this metric, standards are not progressed. A general concern for the objects defined in this section is that it is hard to imagine semantically equivalent objects implemented across a variety of software vendors that would lead to the multiple interoperable implementations necessary for success.

[5] This attribute helps to illustrate another foundational concern of the approach to management in this and related documents. That is, an understanding of the configuration information across time. The management system must know the detail management objects (especially with regard to configuration) across time for each device to assess when the device is in compliance with policy (in the case of this attribute, access policy), and if not, if that policy violation is 'approved'. Abstracting the details, or even putting a level of indirection between the details and the management system makes this analysis more difficult.

Status Objects

EndDct, NodDct and PthDct are all events rather than status changes in a network environment. The important question here is context around the status change, for example:

1. Is there 'flapping' - are the nodes connecting and disconnecting repeatedly?

2. What is the time period for the connects and disconnects?

3. How frequently are the new paths being discovered/changed?

Additional context about configuration changes is often needed to get to the source of a problem.

Setpoint

The single NodSet parameter is very general, making implementation in an operational environment would be difficult. While the details of how to map from this abstract value to something useable have been deferred to a later document, it is important to know that standardization of even the translation of this or many other attributes has historically been problematic. The reason for this is that how a technology is configured and monitored varies not only from vendor to vendor, but can change with software and feature revisions. In order to accurately determine what should be in a NodSet (even in the setting objects defined in section 7.3) one needs to know the following about the device configured:

1. Vendor
2. Model
3. Hardware configuration of the model
4. Software revision (and feature set of the software).
5. Software configuration
6. Firmware
7. In some cases:
    a. Configuration of other elements in the network environment.
    b. Configuration of other software parameters on the system

While not all of these are variables in all conditions, and in fact in many conditions they are not, the variations do exist.

Controls

These are fine as long as they are supported in the device hardware and software.

Section 8.1.2 Network Backup Monitoring

The term 'configuration' is used in a way that is not intuitive. The objects NetAltPth and NetAltNod exist as secondary or tertiary effects of the configuration of one too many network elements. More importantly they are dynamic and can change during the normal course of operation. The NetAltNod is particularly problematic if it is intended to be a listing of all possible paths for each piece of equipment in the network, even a small one. For a path to be useful, it must have a destination. How many potential destinations for an individual element are to be included? How are they specified?

Alarms

AltPthLos and AltPthSw should be specified as to whether it is the routing layer (and which protocol). Further, this is something that is also dynamic. Performance of the network is sometimes considered in making route selection, so even if the absolute number of paths does not change, the details of the path will.

AltNodLos might better be specified if it were clearer. If a node goes down, it will have an impact on many paths. How is this related to AltPthLos?

AltNodSw is conceptually a good idea if it were expressed in the proper level of detail for the routing protocol in question. Without this, if may be hard to ascertain what the actual issue is. A general concern for all these objects is that in networks there are a number of timers that exist to help with route flapping. Even with these timers in place, the number of state transitions and route changes can be significant. For all these objects, the idea of rate of change and absolute number of changes among other factors should be considered. Extant management software understands these conditions in the context of existing standard objects, which is why they should be preferred to recasting them into new abstract objects with the resulting loss of context.

Values and Status

The objects in these sections appear to have the same weakness of those in the alarms section: the potential volume of the events that cause the creation of instances of these objects, the absence in the specification of rate or other factors to give context, and lack of definition of the path.

Section 8.1.3 Network communications failures and degradation monitoring

Before discussing each of the objects, it is important to note a broad problem with this approach. While the introduction talks about per physical link or network level there is no discussion about the following:

1. How are the instances[6] identified (e.g., eth1, eth0, etc.)?
2. How are interface numbering changes dealt with?
3. How are the differences in naming conventions across vendors addressed?
4. How are stacked interfaces – physical interfaces that are divided into multiple logical interfaces – addressed?

Section 8.1.3 discusses the integration of "SNMP MIBs"[7] with the objects in the tables. The practical problems identified in the points above along with incompatible data types, while not

[6] Section 7.2.2 discusses data object construction and in the resource identity definition it is clear given the rest of the context of this document that, when an OID is used (which is not always the case per the spec.) it is not likely to be the same name space as used in the SNMP Framework (see next comment) this is problematic for all objects that come from that namespace.

[7] In the SNMP Framework, there is one, and only one MIB. The name space is divided into MIB Documents that contain one or more MIB Modules. This contiguous name space is a fundamental principle in the SNMP as it also incorporates issues of instance naming point out previously.

impossible to overcome, would be very problematic and expensive. While these comments are raised in this section, they are concerns for many of the objects in this specification.

1. ConnFailTmms – It is not possible to understand this object without additional context.

2. ConnRtryCnt and ConnRtryTmms– This is often configurable per protocol so more context is needed. Further, retries and failures are not always simply a matter of monotonically increasing values. Often they are measured as occurrences per some time unit.

3. ConnFailRtryCnt – Too inadequate of a definition to comment.

4. ConnFailRtryTmms – An excellent concept. As usually implemented, these are not linear times. They are often specified in terms of increasing back off after the detection of a failure in an NMS to avoid unnecessary traffic/load.

Same comment as other sections that contain configuration objects: There does not seem to be a definition in the earlier section of configuration objects as there is for alarm objects for example.

Alarms

1. ConnAlm – Needs ability to specify what type of connection. Additionally, there needs to be a control for hysteresis to avoid too many redundant alarms.

2. ConnFailAlm and ConnFlovAlarm - Excellent objects as long as the context information previously discussed is passed along.

Values

All the objects in this area RsTmms, ConnFailTof, ConnTotTmms, ConnCurTmms, ConnAvTmms, ConnRej, and ConnFlovID are useful objects if context can be passed along. In this case, a unique connection ID would have to be preserved to determine if the same or a different link or route were having difficulty.

Controls

ConnRs needs additional details for further comment.

Section 8.1.4 Communication Protocol Monitoring

The wording of the initial paragraph is a bit confusing. It states:

As discussed in 6.1.4, the following NSM data objects are used for communication protocol monitoring. These are focused on the data protocols, not the network equipment or networking functions. Therefore, these data objects are related primarily to the messages being sent over the networks.

While it is correct that some of the data can be collected directly from the network as opposed to the network element, some objects like buffer overflow alarms would come from the network element. This is not to say that collecting data from direct listening to the network would not be valuable from both an overall monitoring as well as a security perspective. The items in this list are probably more easily collected from the routers or other network equipment.

1. ProtId and ProtVer - Both are generally available from the systems. Same comment as before about use of the term 'configuration'.

2. RescExhPct – This does look like a 'genuine' configuration parameter, but it may need to be qualified by type(s) of resource it is representing. For this and any other alarm of this type, it is often not the absolute value of the usage that gives the best/earliest warning of a problem; it is the rate (and sometimes direction) of change in the utilization of the resource. For example if a system is running at 40% of CPU or memory utilization and the alarm threshold is set to 80%, valuable time might be lost as an attack drives the usage up over what may be several minutes of time.

3. ProtMisAlm – If there is a decision to monitor protocol mismatches, then the system must be configured with controls to avoid too many events[8].

Alarms

There are 8 objects defined in this group, and in addition to the issues of instance correlation to the abstraction layer and across configuration (e.g., CLI) and monitoring (e.g., SNMP) technologies, they require some of the other facilities pointed to in the previous section:

1. Ability to limit the number sent from a device per unit of time.

2. Ability to limit events and cause a back off in the rate of transmission. For example, when an event first occurs, you may want more frequent alerts but if after an hour it has not yet been dealt with, the system should back off.

3. Ability to control absolute number of events sent from a device.

One of the reasons all these rate limits are important for events (in all sections of this specification) is that certain actions that cause events might be made worse by the over reporting by the systems themselves, a DOS by the network on itself.

Values

1. The attributes: MsgDivTmmsAv, MsgDivTmmsMin, MsgDivTmmsMas, MsgCnt, MsgBytAv, MsgBytMin and MsgBytMax would all benefit by indicating the layer of the protocol stack in question as different layers may have different message sizes. To the extent that UDP is used in the network it is especially important to know the Maximum Transmission Unit (MTU) size supported by different parts of the network.

[8] On of the challenges that has been addressed to varying degrees by network equipment and management software vendors over the past two decades is the problem of sending too many alarms/events from network equipment. The suppression of duplicates by the network equipment or throttling back of same events over time helps. Network management software also has evolved to understand specific types of events based on specific SNMP MIB objects to help get to the root cause of the problem. Another impact of the use of the abstraction suggested in this document is that meaningful portions of code would have to be redone.

2. LnkLstAuthOut and LnkLstAuthIn – More definition of this attribute is needed before additional comment is possible – specifically what determines authorized?

3. Need additional detail on LnkLstAvail.

Controls

Both the MsgDivTmmsRs and MsgBytRs attributes are good to have but there are other 'resets' that may be of value beyond these such as a global counter reset to reinitialize all counters.

The reinitialize all counters concept raises and important point. Many counter values (this applies more to 32 bit counters than 64 bit ones) will wrap over time. Network management systems have developed code over the years to address these limitations and the abstract system supported by objects in this document will have to implement similar functions. There are objects in most systems that could be retrieved that would be helpful such as sysUpTime (see RFC 3418):

"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."

By knowing if the counters have wrapped versus the system being rebooted, operators and the software can know how to interpret the value of a counter at a particular moment in time. There are additional counters that should be incorporated. For example, snmpEngineBoots tells operators the number of times the management agent has been restarted and snmpEngineTime lets operators how long since the agent has been restarted. RFC 3411 describes the Architecture for SNMP Management Frameworks.

Section 8.2.1 End System Monitoring

The title of this section is "End system monitoring', yet gateways and data concentrators are listed. Gateways and other communication equipment are not generally regarded as end systems in the data communications environment. End systems would include servers for example.

Configuration settings

Same comment as in other configuration settings sections – these do not seem like configuration settings.

1. EndOI – The exact meaning of this is not clear. Where is the OID assigned? Is that a function of the management software, or is a unique OID created somehow for each system? What happens when networks are merged? Do the OIDs go through a process of conflict resolution?

2. NetOILst – Depending on the nature of the system, the number of open connections that a router or other end system will have can be quite large. As a general rule, it has proven to be impractical to retrieve the entire routing table or TCP Connection Table

from end systems on any regular basis. If this object is intended to be used in time of network stress, that should be noted[9].

3. EndOIList – From the definition provided, it is not possible to distinguish this element from NetOILst. Additional detail is necessary.

4. EndOIRole – This object needs more definition. What is the general objective of the object and what are the accepted roles?

Alarms

There are some general concerns for all alarm objects in the specification based on section 7.3 "High level NSM data type structures". In particular, the alarm structure seems to include information that may be better synthesized by the management application as opposed to the end system[10]. For example, the priority may be better analyzed by the management system. The alarm object type also includes "other", which will be problematic without further specification.

1. DataInvAlm, ReqInvAlm, and CntLAlm would all benefit from additional context information related to the portion of the managed element that is having difficulty. It does not appear that ResourceID would cover all cases as would occur in multiple instances of a routing protocol running or stacked interfaces.
2. AppAlm, AppDataAlm, EndAlm and EndBckAlm also require both additional instance information and details about the type of alarm (such as unable to write to disk, etc.).
3. NetAlm requires some of the controls mentioned previously. They include controls for how often to send an alarm, how many to send, etc.

Values

The intended relationship between Alarms and Values for all sections in the document should be better articulated. Section 7.2.3 states:

All parts of instantiated data objects shall be accessible (according to their access field) to authorized users and applications. This does not imply that all of these parts must be transmitted together, e.g. the value may be transmitted on event, but the other parts only upon direct request.

How are the objects related to each other? What are the valid and invalid combinations? However, the attributes in this section are good elements to collect to the degree instance level context can be preserved, both with the alarm objects in the previous section and the software instance on the device in question.

[9] In general, usage or implementation tips would help with many of the attributes in this document. That is, an extended definition that more precisely states what the object represents (i.e., how it is realized/implemented) and conditions under which retrieval may be advantageous. It should also include usage warnings – for example don't' collect more than N times in any time period due to network or other constraints.

[10] This is a concern form many of the objects in the document. Some seem like straightforward objects that might be retrieved from a router, server, or any other type of managed element in the environment. Others seem to require history, context and other information more likely to be found in a management system. Being clear about what is required from each type of system would likely improve interoperability.

Related to context for these and other alarms is the 'configuration' of the element. This means the values for specific parameters that control the behavior of the end system. For example, what are the default routes a system has been configured with, when were they last changed, who made the change? The correlation of this type of configuration information with faults, security alerts and other types of data retrieved from managed elements is crucial to understanding what is going on in the network. This configuration information must be understood in a machine-specific way, as abstraction would hide important details.

Log

EndLog raises an important question. Many systems have a variety of logging approaches, the most common of which is syslog. Not only do end systems use this facility, but also many network elements (such as routers) support syslog. Some environments have a central logging server with software designed to help rapidly analyze the large amount of data that can come in. There is no definition of a data type for Log in section 7 of the document where other abstract data types are defined.

Section 8.2.2 End System Security Management

1. EndHrdOff and EndHrdOn - Good examples of why the security and management systems should be one in the same thing since they will contain most of the same data. The security system could be viewed as an additional module of the management system. The reason is that for operational reasons, a system may be shut off and knowing it is the result of an intended operation is important. Additionally, if the system if off, it is unclear how it is turned on.

2. EndRs - Has the same issue as the on and off controls above plus more specificity is needed about what resent means.

3. AppOff - Needs information about which instance to 'kill'.

4. EndOpMode and EndConnEst - Both require additional information/clarification as to what these objects are intended to do.

5. EndLogCrt – Useful object, but there may be several logs on a system so this may need an additional parameter to specify which one.

Section 8.3 Intrusion Detection NSM Data Objects

An additional concern for all the objects evaluated in the following sections is that there are many kinds of resources beyond those enumerated that are subject to resource exhaustion. Knowing the details of the hardware and software element and the metrics used to measure the resource would be helpful. In some cases the terms used are different and in some cases they are the same. For example if a network element has been configured to deliver Differentiated Services[11], there may be a problem with an input or output queue that could impact performance

[11] See a series of IETF RFCs on this subject.

of important traffic. Similarly, over saturation of local area network capacity would be another technology-specific area that should be monitored.

Section 8.3.1 Unauthorized Access NSM Data Objects

1. AuthUsrLst – This is an excellent object. In many network environments as they scale, operation personnel use a number of different approaches to control access and privileges. One of the most common is to have managed systems such as routers use TACCAS+. What this means is that the details of the permissions are not stored on each device, but on the TACCAS+ server. While it is not expected that many utilities currently have this environment, as networks are deployed, they may reach the scale where this does become important. As a consequence, the security system may have to participate in this environment and get information about devices from the [access] server as opposed to the device itself. Also, management protocols can incorporate their own access model. SNMP, especially in the v3 administrative framework, has users with roles and other security parameters of interest that should be managed and examined[12].

2. UnAuthAlm –This needs controls settable on the end system to avoid over saturating the environment with duplicate events.

3. UnAuthUsrId – Does this mean access of a general nature or a particular operation for which a known user is not authorized?

4. UnAuthUsrId – “IP Address?” In many environments, users and systems are given access on a per IP basis so it is relevant for this object to retain it. Reporting both the user or system/process attempting access and the IP address/location from which the access was attempted are important.

5. UnAuthUsrCnt and UnAuthTre - Both would be improved if they were expressed over some known time period. Rate implies a rate per some unit of time, but knowing for how long this rate persisted would be helpful.

Section 8.3.2 Resource Exhaustion NSM Data Objects

ConnCnt and ConnSimCnt are most valuable when considered in terms of history/rate and the configured value. It may be helpful in some cases to understand if there are restrictions on type of connection, for example in an HTTP environment, how many connections does a server support.

Alarms

1. ConnExcAlm and ConnExcSimAlm - Both are useful when scoped by the specific alarm type.

[12] Due to the sensitive nature of the environments that are the subject of this and related standards, SNMPv3 is recommended over v1 or v2.

2. IdlTmmsMinAlm and IdlTmmsMaxAlm - Both require some additional information and context. It is not clear what these alarms are intended to convey.

Values

ConnExcMax, ConnExcSimMax and IdlTmms would be more useful if they could be understood over what period of time they are expressed. In a more traditional Network Management System, data are collected at specified intervals and the system keeps track of when data are collected so this information can be calculated by the NMS. Due to the abstraction approach taken for the implementation of these objects, it is not clear that this approach could be taken. To the degree such techniques are possible, they should be captured in some document on best practices.

Section 8.3.3 Buffer Overflow NSM Data Objects

BufOvAlm, BufUnAlm, BufOvCnt, and BufUnCnt are all useful objects if they can be constrained by time as described in the previous section and throttled as described in earlier sections.

BufUsrId is problematic since it may not be possible to identify the ‘user causing’ buffer problems. Indeed, it may take quite a bit of analysis to pinpoint the reason for the overflow.

Section 8.3.4 Tampered/malformed PDUs

All of the objects in this group are subject to the same comments as previously made with regard to time frame the alert/alarm represents and lack of specifics of the technology. Knowing the protocol(s) in question (e.g. TCP, UDP, SNMP, HTTP, etc) would be very helpful in understanding the nature of the problem. Analysis of certain packet types and size distributions is also missing in this section.

Section 8.3.5 Physical Access Disruption

1. PwrLosAlm – Device level implementation may be problematic – except in the case of an orderly shut down. It would be possible to infer this from some other systems but they would only be able to indicate reach ability, not necessarily power state.

2. PwrOnAlm – It and PwrLosAlm (to the degree it is implemented) need to have what has been termed in the network environment ‘source side notification suppression’, where the managed element can be configured to control how many and often certain types of alarms are sent[13].

3. ComLosAlm, ComOnAlm and DoorOpAlm - All require the throttling/control mechanisms described previously.

[13] Many technologies make distinctions between events and alarms that could be usefully applied in the framework the management objects in this document will exist in. Those distinctions should then be reflected in a revised object list for this document.

4. PwrLosCnt and ComLosCnt – Same comments as previous for similar objects – need to know what unit(s) of time the counts are for or the management model that would provide this information.

Section 8.3.6 Invalid network access

It is not clear how TrfFrqSet and TrfVolmSet (for traffic frequency and volume) relate to the title of this section: "Invalid network access". While a variety of attacks might result in too much traffic, or too much traffic of a certain type, almost any limit object in this document could be said to indicate a potential threat monitor. Further clarification of these objects would be helpful. If there were limits based on source network or IP address, then they might be clearer.

All the previous comments related to other alarms and values apply to the alarms and values objects in this section.

Section 8.3.7 Coordinated Attacks

1. SynTmms and AtkTmms – The definitions of these objects are not clear, more information is needed.

2. AtkCnt – To the extent this object/configuration parameter is modified by AtkTmms, this is a good example of how time should be associated with different counters.

Alarms

1. SynAlm – Needs additional detail in the definition to make meaning and method of implementation clear.

2. AtkAlm – If it is known that there is a coordinated attack at sufficient detail to send this alarm, then more information should be sent with the alarm to aid defensive measures[14].

Values

1. SynId – Too little detail – needs more information in the definition.

2. AtkTyp – If there is a list of known attack types, they should be enumerated with this object.

Recommended Instrumentation Additions

The integration of information from different sources of data such as the network, applications, power generation, transmission and distribution resources is critical. It is through this integration that one will get the full picture of the operational state of the environment.

[14] Established networking/management technologies have methods by which supporting information is supplied with different types of alarms/events. The alarm structure defined in this document does not seem to have any such facility will reduce the value of alarms.

Data from Network Connected Devices

Additional network related details may further the goal of creating a complete operational picture of the network environment. To fully understand this operational picture, of which security is a key element, un-abstracted network technology details are needed. Here are some examples:

- Media – Types of media as well as the physical topology.
- Routing Protocols – It is difficult to understand the operational state of an IP network without unobstructed details of the routing system. There are a number of standards available from which the management system could collect these data elements.
- The DNS is another critical infrastructure element that should be carefully monitored and controlled. A number of these systems also have instrumentation from which important information can be collected.
- Layer 2 information – Not all attacks and operational problems are immediately visible without information about protocols below the TCP/IP layers.
- Specific Details of Resources and End Systems – This includes information about disks, network interfaces, etc.
- Application Specific Information - Servers, etc.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

1024421

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com