IEC/TS 62351-7

Edition 1.0 2010-07

TECHNICAL SPECIFICATION

colour inside

**Power systems management and associated information exchange –
Data and communications security –
Part 7: Network and system management (NSM) data object models**

IEC/TS 62351-7:2010(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TS 62351-7

Edition 1.0 2010-07

TECHNICAL SPECIFICATION

Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-88912-050-5

CONTENTS

FOREWORD 4
1 Scope 6
2 Normative references 6
3 Terms and definitions 6
4 Glossary of terms and definitions 6
5 Background of network and system management (NSM) requirements (informative) 6
5.1 Objectives of IEC NSM standards 6
5.1.1 Scope of end-to-end security 6
5.1.2 End-to-end security measures 7
5.1.3 Security purposes 8
5.1.4 Role of network and system management (NSM) in end-to-end security 8
5.1.5 Scope of the NSM standard 10
5.2 Current lack of coherent information infrastructure 10
5.3 Intrusion detection systems (IDS) 12
5.3.1 ISO/IEC 18043 IDS guidelines 12
5.3.2 Intrusion detection system (IDS) concepts 13
5.3.3 IDS: Passive observation techniques 14
5.3.4 IDS: Active security monitoring architecture with NSM data objects 15
5.4 Network and system management (NSM) concepts 15
5.4.1 IETF and ISO network management standards 15
5.4.2 ISO NSM categories 16
5.4.3 Simple network management protocol (SNMP) 16
5.4.4 Management information bases (MIBs) 16
5.4.5 NSM “data objects” for power system operations 17
6 Security and reliability NSM requirements for power system operations (informative) 17
6.1 NSM requirements: Monitoring and controlling the networks and protocols 17
6.1.1 Network configuration monitoring and control 17
6.1.2 Network backup monitoring 18
6.1.3 Network communications failures and degradation monitoring 18
6.1.4 Communication protocol monitoring 18
6.2 NSM requirements: Monitoring and management of end systems 19
6.2.1 Monitoring end systems 19
6.2.2 Security control and management of end systems 20
6.3 NSM requirements: Intrusion detection functions 20
6.3.1 Detecting unauthorized access 20
6.3.2 Detecting resource exhaustion as a denial of service (DoS) attack 21
6.3.3 Detecting buffer overflow DoS attacks 21
6.3.4 Detecting tampered/Malformed PDUs 22
6.3.5 Detecting physical access disruption 22
6.3.6 Detecting invalid network access 22
6.3.7 Detecting coordinated attacks 23
7 NSM abstract data types 23
7.1 Abbreviated terms 23
7.2 NSM data object constructs 24

7.2.1 NSM data object fields 24
7.2.2 Construction of data objects 25
7.2.3 Access to data objects 26
7.3 High level NSM data type structures 26
7.3.1 Opaque (not known / not specified / special) 30
8 NSM abstract data objects 30
8.1 Communications health NSM data objects 30
8.1.1 Network configuration monitoring and control 30
8.1.2 Network backup monitoring 31
8.1.3 Network communications failures and degradation monitoring 32
8.1.4 Communication protocol monitoring 33
8.2 End system health NSM data objects 33
8.2.1 End system monitoring 33
8.2.2 End system security management 35
8.3 Intrusion detection NSM data objects 35
8.3.1 Unauthorized access NSM data objects 35
8.3.2 Resource exhaustion NSM data objects 35
8.3.3 Buffer overflow NSM data objects 36
8.3.4 Tampered/malformed PDUs 36
8.3.5 Physical access disruption 37
8.3.6 Invalid network access 37
8.3.7 Coordinated attacks 38
Bibliography 39

Figure 1 – Comparison of NSM data objects with IEC 61850 objects 9
Figure 2 – Management of both the power system infrastructure and the information infrastructure 9
Figure 3 – Power system operations systems, illustrating the security monitoring architecture 12
Figure 4 – Information exchange between applications: generic communication topology 13
Figure 5 – Active security monitoring architecture with NSM data objects 15
Figure 6 – Alarm structure 26
Figure 7 – Status structure 27
Figure 8 – Measurement structure 27
Figure 9 – Setting structure 28
Figure 10 – Array 28
Figure 11 – Table 29
Figure 12 – Control hardware 29
Figure 13 – Control software 30

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 7: Network and system management (NSM) data object models

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-7, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/1003/DTS	57/1062/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

A list of all parts of the IEC 62351 series, under the general title: *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 7: Network and system management (NSM) data object models

1 Scope

Power systems operations are increasingly reliant on information infrastructures, including communication networks, intelligent electronic devices (IEDs), and self-defining communication protocols. Therefore, management of the information infrastructure has become crucial to providing the necessary high levels of security and reliability in power system operations. Using the concepts developed in the IETF simple network management protocol (SNMP) standards for network management, IEC/TS 62351-7 defines network and system management (NSM) data object models that are specific to power system operations. These NSM data objects will be used to monitor the health of networks and systems, to detect possible security intrusions, and to manage the performance and reliability of the information infrastructure.

The NSM data objects use the naming conventions developed for IEC 61850, expanded to address NSM issues. These data objects, and the data types of which they are comprised, are defined as abstract models of data objects. The actual bits-and-bytes formats of the data objects will depend upon the mapping of these abstract NSM data objects to specific protocols, such as IEC 61850, IEC 60870-5, IEC 60870-6, IEC 61968/IEC 61970 (CIM), web services, SNMP or any other appropriate protocol. Those mappings will need to be standardized in separate documents.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC/TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

3 Terms and definitions

For the purposes of the present document, the terms and definitions given in IEC/TS 62351-2 apply.

4 Glossary of terms and definitions

See IEC/TS 62351-2.

5 Background of network and system management (NSM) requirements (informative)

5.1 Objectives of IEC NSM standards

5.1.1 Scope of end-to-end security

End-to-end security encompasses not only deliberate attacks but also inadvertent actions.

This statement is crucial to understanding the scope of this standard. Although some definitions of “security” just include the protection of systems against the deliberate attacks of terrorists or cyber hackers, often more damage is done by carelessness, equipment failures and natural disasters than by those deliberate attacks. Therefore, in this standard, “security” covers all hazards, including deliberate attacks, inadvertent mistakes, equipment failures, software problems and natural disasters. For the security and reliability of power system operations, it does not matter whether a problem was caused by a deliberate attack or by an inadvertent action.

In addition, many of the same measures that could be used against deliberate attacks can be used against inadvertent actions. Therefore, it is useful and cost-effective to address both types of security threats with the same types of security measures.

5.1.2 End-to-end security measures

IEC/TS 62351-3 to IEC/TS 62351-6 address security measures for communication protocols. End-to-end security entails a much larger scope than just the authentication of users and the encryption of these protocols. End-to-end security involves security policies, access control mechanisms, key management, audit logs, and other critical infrastructure protection issues. It also entails securing the information infrastructure itself.

As discussed in IEC/TS 62351-1, security threat agents include:

a) Inadvertent: Threat agents which may cause inadvertent “attacks” on systems:
   - careless users;
   - employees who bypass security;
   - safety system failures;
   - equipment failures;
   - natural disasters.

b) Deliberate: Threat agents which undertake deliberate attacks:
   - disgruntled employee;
   - industrial espionage agents;
   - vandals;
   - cyber hackers;
   - viruses and worms;
   - thieves;
   - terrorists.

The key point is that the overall security of power system operations is threatened not only by deliberate acts of terrorism but by many other, sometimes deliberate, sometimes inadvertent threats that can ultimately have more devastating consequences than direct espionage.

As noted in IEC/TS 62351-1, securing protocols using IEC/TS 62351-3 to IEC/TS 62351-6 essentially provides authentication and (for some protocols) encryption over the communications link, covering 3 of the 4 security requirements: integrity, confidentiality and non-repudiation. These very important security measures still, however, leave serious gaps:

– First, they cover only the protocols over the communications link, and do not address the end users and end equipment. Masquerading users, equipment failures or undetected intrusions can disrupt operations even if the data exchanges are continuing correctly.
– Second, they do not address denial of service. Denial of service can take many forms, from slowed data exchanges, failures of equipment, faults in communication paths, sporadic or decreased availability, interference and theft.

Although the main objective of security measures may be to prevent security attacks, security measures cannot be entirely preventative. If only prevention were attempted, then when (there is always a when) an attacker does manage to penetrate a periphery, they would have complete freedom to do whatever damage they wanted to. Therefore, “prevention” of attacks should be viewed as both deterrence and delay of attacks. In addition, security protection needs to be provided to counter attacks that were not deterred.

5.1.3 Security purposes

The purposes for security protection are often described as 5 layers, with security measures addressing one or more of these layers:

- Deterrence and delay, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. This is the primary defence, but should not be viewed as the only defence.
- Detection of attacks, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort.
- Assessment of attacks, to determine the nature and severity of the attack. For instance, has the attack breached the confidentiality of private data, or is the attack more of a nuisance such as the printer not being available.
- Communication and notification, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort.
- Response to attacks, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

5.1.4 Role of network and system management (NSM) in end-to-end security

End-to-end security involves far more than encryption or authentication, which are the primary security methods. As discussed in IEC/TS 62351-1 and shown in Figure 1, the entire information infrastructure must be made secure and reliable in order to provide security and reliability of power system operations. Figure 2 shows the management of both the power system infrastructure and the information infrastructure.

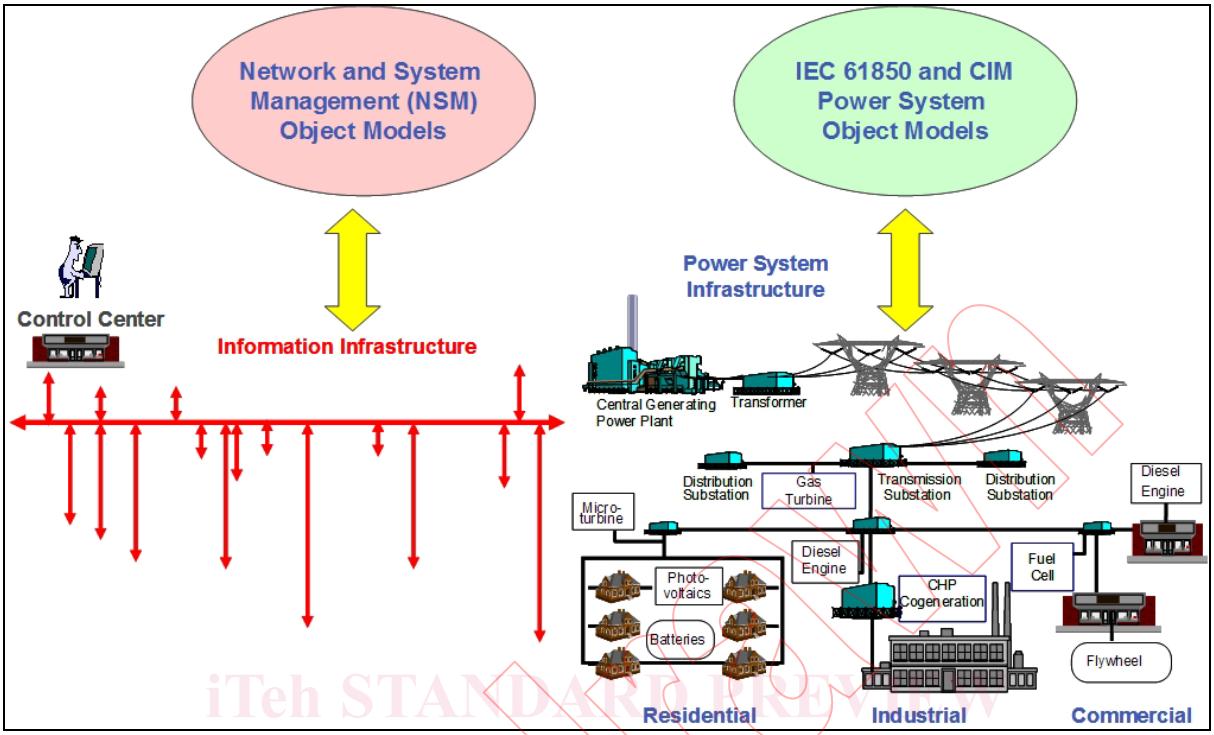

Figure 1 – Comparison of NSM data objects with IEC 61850 objects

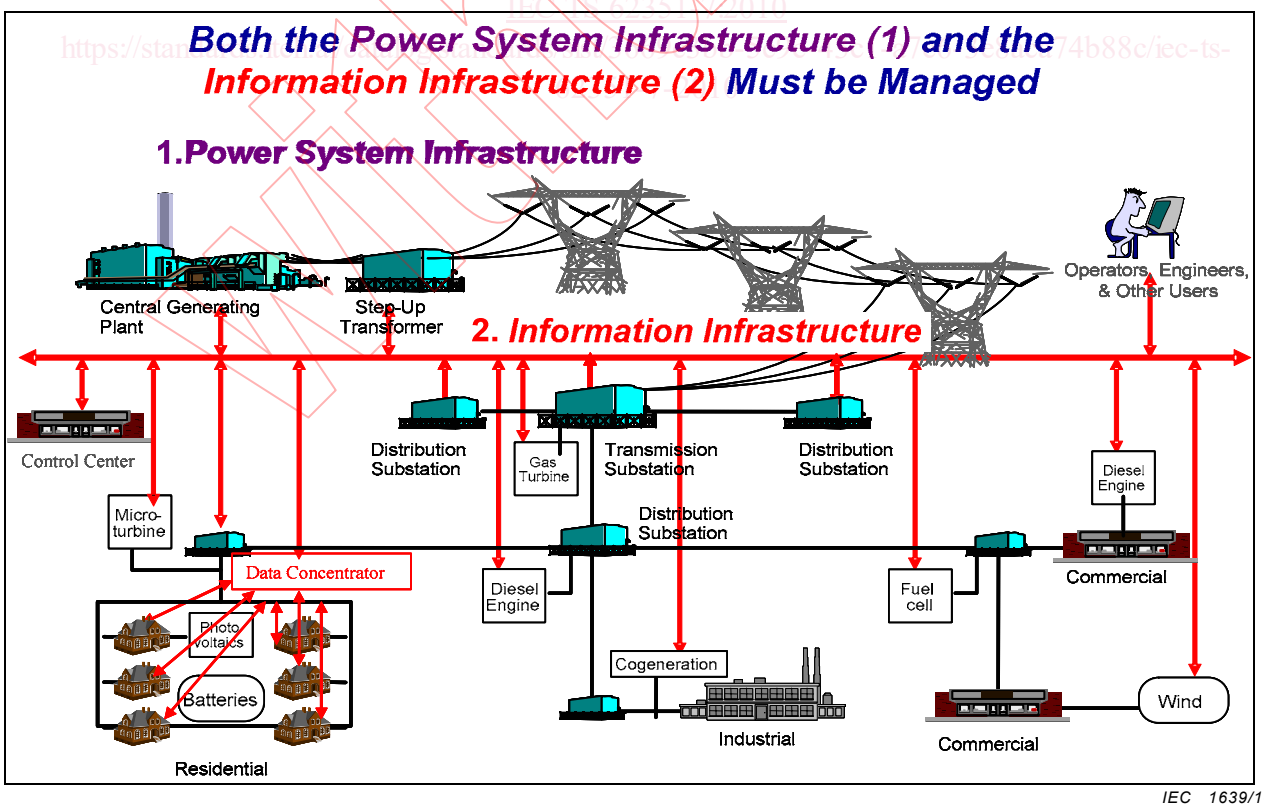

Figure 2 – Management of both the power system infrastructure and the information infrastructure

Not all of these security and reliability requirements can be filled by network and system management (NSM), but many of them can be ameliorated. Specifically, the following functions can be provided by NSM:

- Monitoring the status of software applications, hardware equipment, and communications. This status monitoring can provide notification of changes, such as equipment failures, abnormal configuration changes, software “crashes” or failures, temporary communication disruptions, and permanent communication failures.
- Monitoring the performance of systems and communications. This performance monitoring can record data traffic conditions, software application performance changes, data throughput changes, performance results from communication configuration changes, etc.
- Intrusion detection. In addition to obvious intrusions, this detection must be sensitive to “normal” conditions in order to attempt to detect subtle changes in conditions which might signal an intrusion. This intrusion detection would utilize the information from the status and performance monitoring.
- Configuration management. The configuration of communications networks and equipment can be managed, either by establishing automatic changes based on events (e.g. move to backup channel if the primary channel fails), or by manually changing the configuration, such as taking one piece of equipment out of service and replacing it with another.

5.1.5 Scope of the NSM standard

The scope of the IEC NSM standard includes the following requirements.

- Monitoring communications networks and end equipment in operational environments, with the purpose of detecting possible attacks, including attacks against confidentiality, integrity, denial of service, and non-repudiation. This monitoring covers performance, configuration, faults, and security. The functions supported by this monitoring include equipment failure/fault detection, performance assessment, certificate assessment, intrusion detection, audit logging, access control, anti-virus protection, backup and remote monitoring of physical security.
- Controls for communication networks and end equipment, with the purpose of preventing or mitigating possible attacks, including attacks against confidentiality, integrity, denial of service, and non-repudiation. The functions supported by these controls include running diagnostics, re-configuration, re-start and application program control.

The end-to-end security issues NOT covered by these NSM standards include:

– security policies;
– identity establishment of users and equipment;
– credential establishment;
– certificate management, such as certificate establishment and certificate revocation;
– physical security measures such as fences, gates, video surveillance, except for the monitoring and control of the equipment used for physical security.

5.2 Current lack of coherent information infrastructure

The information infrastructure in power operations is not typically treated as a coherent infrastructure, but is viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols. Often SCADA systems perform some minimal communications monitoring, such as whether communications are available to their remote terminal units (RTUs), and then they flag data as “unavailable” if communications are lost. However, it is up to the maintenance personnel to track down what the problem is, what equipment is affected, where the equipment is located, and what should be done to fix the problem. All of this is a lengthy and ad hoc process. In the mean time, the power system is not being adequately monitored, and some control actions may be impossible. As the analysis

of the August 14, 2003 blackout showed, the primary reason behind the blackout itself was the lack of critical information made available to the right user at the right time.

Every utility is different in what information is available to its maintenance staff. Telecommunication technicians are generally responsible for tracking down any microwave or fibre cable problems; telecommunication service providers must track their networks; database administrators must determine if data is being retrieved correctly from substation automation systems or from geographical information system (GIS) databases; protocol engineers must correct protocol errors; application engineers must determine if applications have crashed, have not converged or are in an endless loop; and operators must filter through large amounts of data to determine if a possible “power system problem” is really an “information system problem”.

In the future, the problem of information management will become increasingly complex. SCADA systems will no longer have exclusive control over the communications to the field, which may be provided by telecommunication providers, or by the corporate networks, or by other utilities. Intelligent electronic devices (IEDs) will have applications executing within them whose proper functioning is critical to power system reliability. Field devices will be communicating with other field devices, using channels not monitored by any SCADA system. Information networks in substations will rely on local “self-healing” procedures which will also not be explicitly monitored or controlled by today’s SCADA systems.

Security and reliability NSM data objects need to be defined that are specific for the power industry. These NSM data objects will support communications network integrity, system and application health, Intrusion detection systems (IDS), firewalls, and other security/network management requirements that are unique to power system operations. The basic elements of power system operations system with the addition of a security monitoring architecture are shown in Figure 3.