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

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.
If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.
Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

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 It also gives information on projects, withdrawn and replaced publications.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

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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

PRICE CODE W

ICS 33.200

ISBN 978-2-88912-050-5

® Registered trademark of the International Electrotechnical Commission

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

CONTENTS

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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 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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

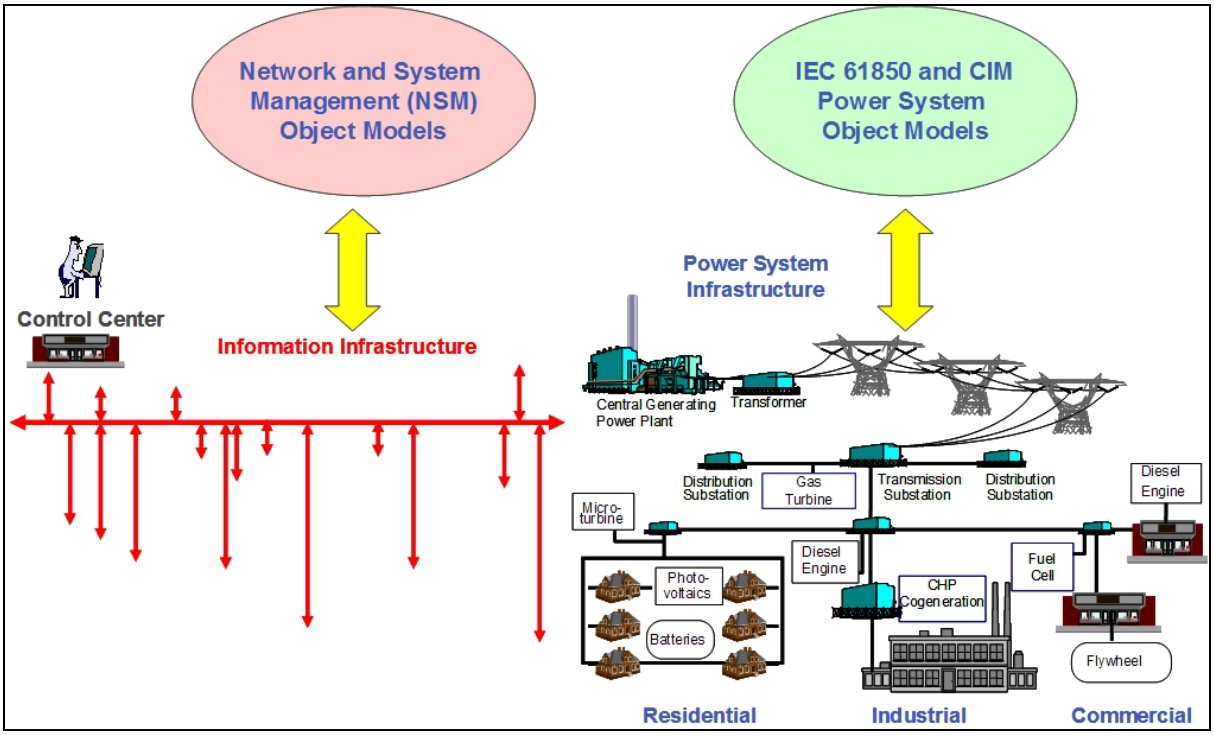

Figure 1 – Comparison of NSM data objects with IEC 61850 objects

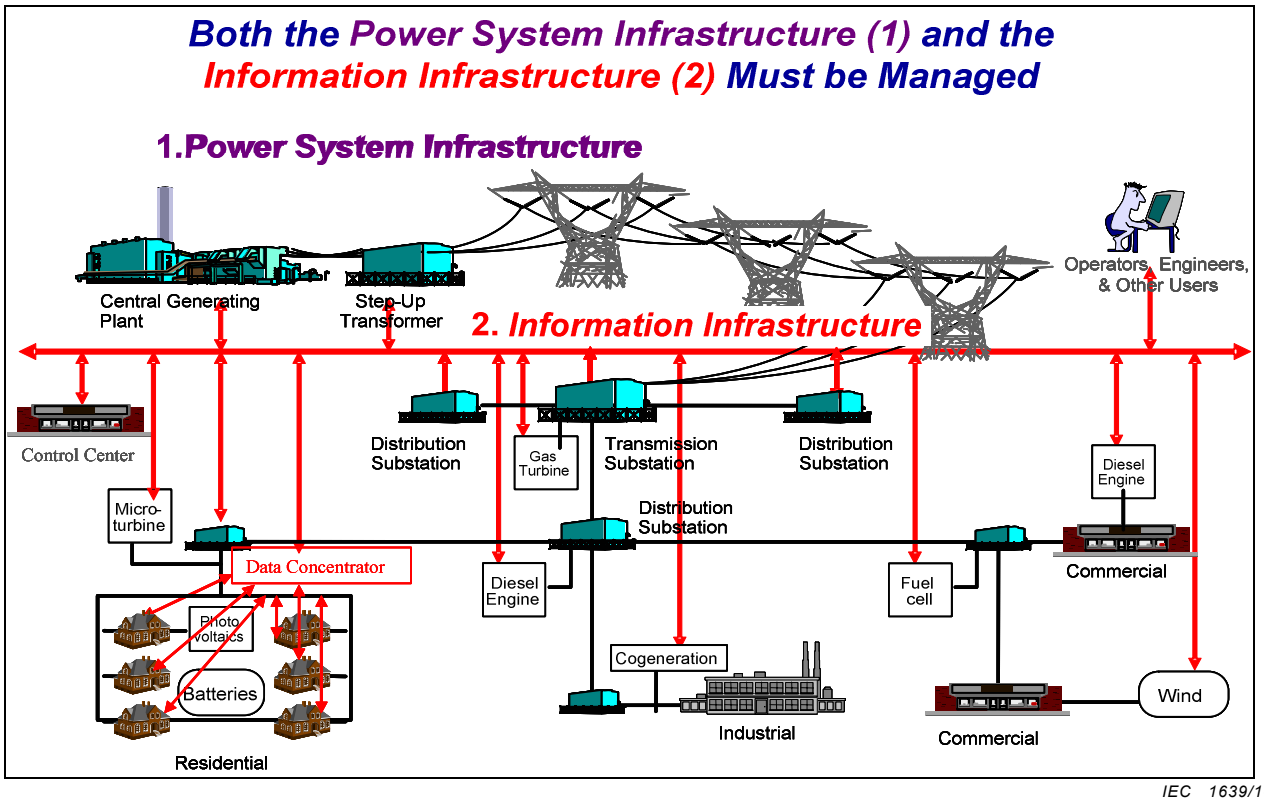

Figure 2 – Management of both the power system infrastructure and the information infrastructure

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

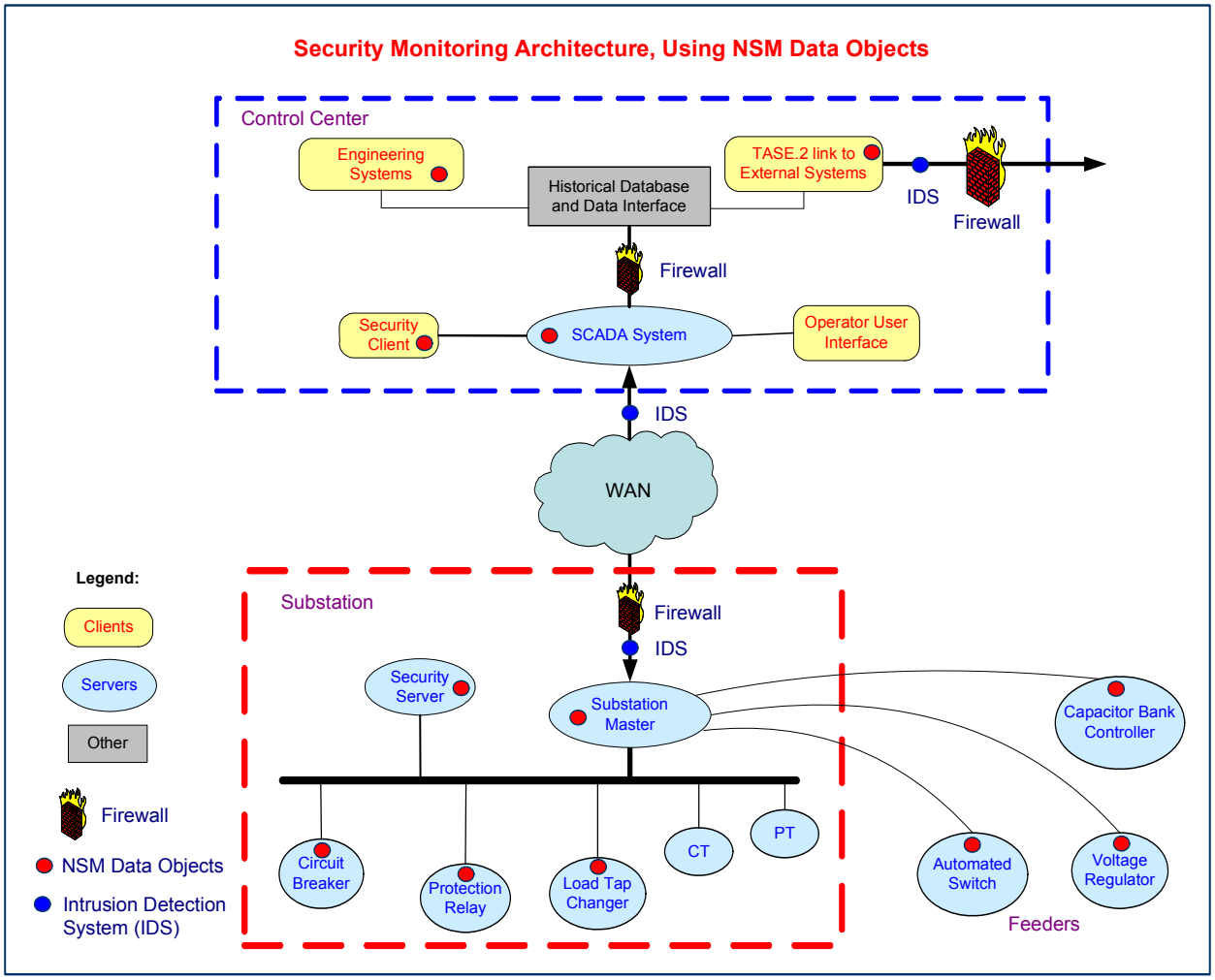

Figure 3 – Power system operations systems, illustrating the security monitoring architecture

The security and reliability requirements that the NSM data objects will fulfil include the types of monitoring and control discussed in the following subclauses.

5.3 Intrusion detection systems (IDS)

5.3.1 ISO/IEC 18043 IDS guidelines

ISO/IEC 18043 provides guidelines for effective selection, deployment and operations of intrusion detection systems. In its Introduction, it states:

"Organizations should not only know when, if, and how an intrusion of their network, system or application occurs, they also should know what vulnerability was exploited and what safeguards or appropriate risk treatment options (i.e. risk transfer, risk acceptance, risk avoidance) should be implemented to prevent similar intrusions in the future. Organizations should also recognize and deflect cyber-based intrusions. This requires an analysis of host and network traffic and/or audit trails for attack signatures or specific patterns that usually indicate malicious or suspicious intent. In the mid-1990s, organizations began to use intrusion detection systems (IDS) to fulfil these needs. The general use of IDS continues to expand with a wider range of IDS products being made available to satisfy an increasing level of organizational demands for advanced intrusion detection capability.

In order for an organization to derive the maximum benefits from IDS, the process of IDS selection, deployment and operations should be carefully planned and implemented by properly trained and experienced personnel. In the case where this process is achieved, then

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

IDS products can assist an organization in obtaining intrusion information and can serve as an important security device within the overall information and communications technology (ICT) infrastructure."

5.3.2 Intrusion detection system (IDS) concepts

Cyber security against deliberate or inadvertent attacks is a critical aspect of network and system management. This cyber security covers not only the security threats aimed at the data exchanges between systems, but also the security threats within systems due to the "intrusion" of erroneous messages and/or malicious code.

For data exchanges, identity establishment and authentication are key security capabilities for ensuring integrity and non-repudiation. Encryption techniques provide security for confidentiality. None of these methods provide much security for availability: in which denial of service (DoS) attacks can cause data exchanges between systems to become less available, slower or totally unavailable.

For internal system cyber security, one of the key security mechanisms is intrusion detection systems (IDS). These IDSs monitor (either "passively" or "actively") the traffic on networks, and, depending upon their capabilities, attempt to determine if some traffic is a security risk, including whether DoS attacks are taking place. NSM data objects can assist IDSs in avoiding or minimizing denial of service (DoS) attacks and other security intrusions.

Many different methods can be implemented to detect security-related intrusions in networks and systems. For end-to-end security, the entire communication path between applications needs to be evaluated, including through intermediate systems (IS), and can be illustrated with the model shown in Figure 4.

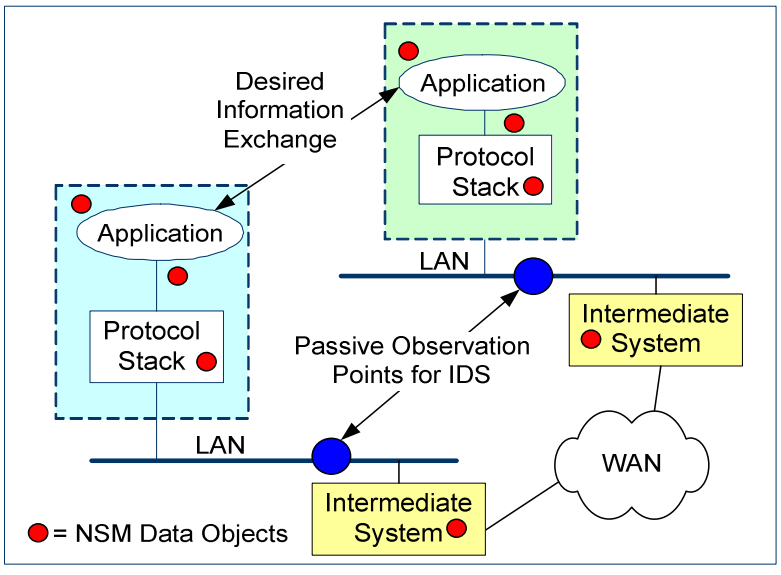

Figure 4 – Information exchange between applications: generic communication topology

The simplified diagram depicts two applications attempting to exchange information. In this diagram, in order to exchange information, the information needs to be:

- transmitted through a local communication stack;
- transmitted from the local communication stack onto a local area network (LAN);
- routed/bridged into a wide area network (WAN) via an intermediate system (IS);
- received by a remote IS;

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

- transmitted by the remote IS onto the remote application's LAN;
- received by the remote application's communication stack;
- delivered to the remote application for processing.

Each of these locations could provide information on possible intrusion detections, including the following types of integrity, confidentiality, availability and non-repudiation security threats:

– resource exhaustion or "significant" performance impacts due to unexpectedly large number of messages being sent, inadvertently or deliberately, which prevent or delay legitimate messages from being received;

– buffer overflows, caused either by "mistakes" in forming messages or by malicious attacks to disrupt system operations;

– PDUs (packets) that are (inadvertently) malformed or have been (deliberately) tampered with;

– invalid network access attempts by messages with unauthorized IP addresses or port requests;

– invalid application access attempts.

Two basic methods exist for IDSs: passive observation techniques and active security monitoring. These are discussed in the following subclauses.

5.3.3 IDS: Passive observation techniques

Passive observation techniques (i.e. requiring no modifications to the IS, COMM stack, or application) require only the addition of "network based IDS" monitors – existing equipment and networks do not need to be modified, thus making these security upgrades easier and less expensive to implement. For this reason, passive IDSs are the preferred approach when considering systems and equipment which are already installed or will use "non-IDS" end equipment.

Figure 4 illustrates two passive observation points in the local and remote networks, shown as two blue circles.

Purely passive IDSs have limited ability to detect intrusions since they may not be "aware" of what normal traffic might be in typical power system operations. However, in addition to these passive IDSs, NSM data objects can be implemented in systems which house the applications and communication stacks, as well as in the intermediate systems (IS) (see the many red dots in Figure 4). These NSM data objects would provide additional intelligence to determine if an attack is underway, what type of attack is taking place, and the time of the critical events.

The NSM data objects in a legacy system would simply include available information that could be sent as additional data using the existing protocols. Often this data is available but either ignored or stored in a local log as an "error". The key is to identify the important, but available data, and provide it to the IDS or to a security system.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

5.3.4 IDS: Active security monitoring architecture with NSM data objects

Active security monitoring involves designing the networks and the end systems with security monitoring as part of the design criteria. Rather than relying on what error checking is available in legacy systems, these systems include in their design the ability to identify and provide additional security information to a “security client”, including information on anomalous events, unauthorized messages, data possibly related to DoS attacks, etc.

In this active security monitoring architecture, each layer in the protocol stack would monitor for possible security attacks, and many applications would provide key error and failure data. A security provider would manage the NSM data objects, possibly setting appropriate thresholds, limits, and other parameters in order to fine-tune the response to more closely fit each power system operational environment. Upon the detection of an anomaly, the NSM data would be sent to the security client for additional analysis (see Figure 5).

This architecture is similar to the SNMP and RMON architectures. However, this does not imply that the SNMP formats will necessarily be used to transmit the NSM data: the NSM data objects would be implemented using whatever protocol is being used for other types of communications.

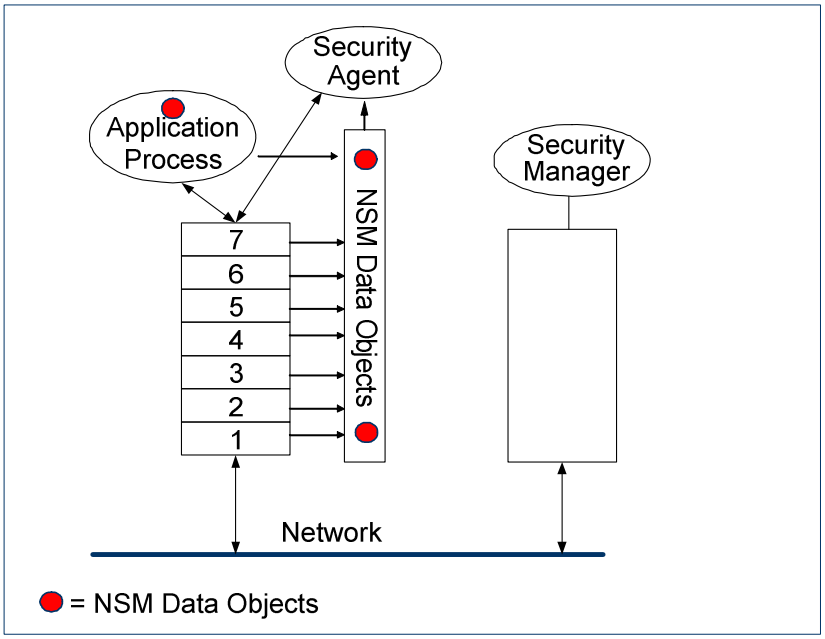

Figure 5 – Active security monitoring architecture with NSM data objects

5.4 Network and system management (NSM) concepts

5.4.1 IETF and ISO network management standards

The technology industry has developed two network management technologies: simple network management protocol (SNMP) for the internet-based functions (standardized by the IETF), and common management information protocol (CMIP) as an ISO standard.

In both standards, management information base (MIB) objects must be specified representing the state of different equipment, applications, and systems. Although some MIB objects are generic enough for typical network equipment to be used by the power industry, many specialized MIB objects will need to be developed to represent some of the very specialized equipment and special environments found in power system operations.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

5.4.2 ISO NSM categories

Network management involves many different aspects, but has been organized by the ISO into 5 areas:

- performance management;
- configuration management;
- accounting management;
- fault management;
- security management.

Of these 5 areas, only accounting management is not directly associated with end-to-end security. The other 4 areas are either directly or indirectly involved in security. For instance, if an equipment failure or a careless parameter change causes degradation of performance, then the reliability of power system operations may be affected; or a change in network configuration could result in a single point of failure that is not recognized until that failure occurs; or an undetected intrusion causes time-sensitive data exchanges to slow down and not reach their destinations in a timely manner.

5.4.3 Simple network management protocol (SNMP)

The simple network management protocol (SNMP) was developed by the IETF as the protocol for transmitting MIBs over the Internet. Many systems use SNMP internally as well. However, MIBs do not need to be transmitted by SNMP; any protocol can be used. In this standard, no explicit protocol is identified for transmitting the MIBs. This means that the MIB data may be transferred via whatever protocol is being used, using whatever mapping to objects is appropriate.

Some systems and equipment do include SNMP. In these cases, the MIBs could be mapped to SNMP directly.

5.4.4 Management information bases (MIBs)

Management information bases (MIBs) are used to define what information is needed to manage the information infrastructure as securely and reliably as the power system infrastructure is managed.

Once the security and reliability information requirements are defined, they can be structured as abstract objects, and formatted as standardized as management information base (MIBs) to be compliant with information industry (i.e. IETF's simple network management protocol - SNMP) standards. These MIBs are the information infrastructure equivalent to the 61850 object models of the power system infrastructure. In essence, managing the information infrastructure is as crucial to the secure and reliable operation of the power system as any encryption or access management security schemes. Just as power system information (defined in IEC 61850 and in IEC 61970) is used to manage the power system, management information base (MIBs) information can be used to manage the information systems.

The IETF and many mainstream vendors of network and system products have developed specific MIBs for their products, with the basic assumption that these products will be used over the Internet or an Intranet based on IETF technologies. These should be used where they exist.

However, many products used in power system operations are not expected to (nor should they) be used over open networks, and have therefore not developed or implemented IETF MIBs for network management. These products and systems generally rely on simple monitoring of communication connections by the SCADA systems.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

5.4.5 NSM "data objects" for power system operations

The NSM "data objects" identified in this standard fill the gap between the existing simple SCADA communications monitoring and the desired secure and reliable information infrastructure for power system operations. "Data objects" are abstract data elements that can be subsequently mapped to different protocols, including IEC 61850, IEC 60870-5, IEC 60870-6 (TASE.2) and enterprise protocols such as SNMP.

This standard specifies the abstract data objects but does not specify the protocols that they may be mapped into. Annexes are planned to provide some common mappings.

It also does not specify the actions that could or should be taken upon receiving an NSM alarm or anomaly: those actions are considered to be implementation-specific and are outside the scope for this standard.

6 Security and reliability NSM requirements for power system operations (informative)

6.1 NSM requirements: Monitoring and controlling the networks and protocols

6.1.1 Network configuration monitoring and control

Typical network management involves monitoring and controlling the communication network configuration. Most vendors of enterprise-level network equipment provide some degree of control. Where these networks are used in power system operations, those control capabilities can be used. However, many communication "networks" used in power system operations are not configured as typical networks or with enterprise-level network capabilities, and therefore do not include typical network management control capabilities. Sometimes a few basic network management capabilities are included in SCADA systems, but are generally proprietary.

The following are the NSM requirements related to monitoring and controlling the configuration of a network. Conceptually, each entity in the network (either a "network node" or an "end device" or a nested "sub network") will contain this information for itself: depending upon the implementation, this information can be "downloaded" from another site or can be "automatically acquired"; however, it is available for viewing, uploading, etc.

The following items are examples of data to be monitored for network configuration monitoring and controlling.

- Network configuration information, including what end systems are connected on what network paths. Backup and alternative paths should also be included. Although some implementations could pre-load the configuration data objects, they should be visible to authorized users.
- Power on/off commands to network equipment. This is a "hard" power disconnect performed by some external system.
- Reset command to network equipment. This is a "soft" command.
- Switching commands to network equipment for changing paths to devices.
- Setting or updating the access control list.
- Setting parameters and sequences for automated network actions.
- Automated actions in response to events, such as reconfiguration of the communications network upon equipment failure.
- Establishing primary and, optionally, secondary paths to each end device.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

6.1.2 Network backup monitoring

In addition to monitoring the network equipment, it is crucial to determine if the network can provide the performance it is designed for. Specifically, the status of alternate paths and backup equipment needs to be monitored to ensure that they are available to handle failures, degraded communication links, and deliberate removal of the primary routes for maintenance or other purposes.

The network backup monitoring requirements include:

- determining status of backup equipment, including ability to be automatically switched to it;
- determining the status of alternate communication links, including the available bandwidth if they were switched to them;
- detecting network equipment failovers to backup equipment;
- detecting switching to alternate or backup communication links;
- detecting the status of backup or spare equipment for use in failovers;
- logging of status and times of all failovers and use of backup equipment.

6.1.3 Network communications failures and degradation monitoring

Network management involves monitoring the state of the communications networks, primarily for equipment and communication failures. Most enterprise-level network equipment from mainstream vendors already includes SNMP MIBs for monitoring these networks. However, most communication networks used in power system operations do not use these types of mainstream networking equipment since often there is no “network” involved – only point-to-point low-speed links between the control centre and each substation. Even where networks are involved, they are often handled more as sets of fixed links rather than true networks.

Therefore, if a specific implementation includes mainstream networking equipment with SNMP MIBs that covers some of the following items, these should be used if possible. For other implementations and for items not covered by mainstream vendor MIBs, data objects need to be developed. These data objects can then be implemented where appropriate.

The network communication failure and degradation monitoring requirements include:

- detecting network equipment permanent failures;
- detecting network equipment temporary failures and/or resets;
- detecting communication link failures;
- detecting communication link degradation or lower than expected throughput;
- detecting network routing degradation or lower than expected throughput;
- logging equipment and communication link failures and degraded conditions.

6.1.4 Communication protocol monitoring

Monitoring of the communication protocols that are being used over the network is also critical. Some of this monitoring can be performed by routers, gateways, firewalls and other systems through which the protocols are passed. 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.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

The communication protocol monitoring requirements include:

- detecting communication protocol version and status;
- detecting mismatches of differing protocol versions and capabilities;
- detecting tampered/malformed protocol messages;
- detecting inadequately synchronized time clocks across networks;
- detecting resource exhaustion forms of denial of service (DOS) attacks;
- detecting buffer overflow DOS attacks;
- detecting physical access disruption such as loss or degradation of connectivity;
- detecting invalid network access;
- detecting invalid application object access/operation;
- supporting broader ability to detect coordinated attacks across multiple systems;
- collecting statistical information from network equipment:
  - determining average message delivery times, slowest, fastest, etc.
  - counting number of messages, size of messages;
- providing audit logs and records;
- detecting the primary and, optionally, secondary paths to each end device.

6.2 NSM requirements: Monitoring and management of end systems

6.2.1 Monitoring end systems

End systems may be intelligent electronic devices (IEDs), remote terminal units (RTUs), substation masters, or any equipment with built-in computer or microprocessor processing capability.

Monitoring of these end systems involve a combination of internal and external assessment of their health. Internal assessments can be more precise in detecting anomalies, while external assessments can determine their state in situations in which the application or end system is not capable of assessing itself. Internal assessments can be performed by applications which directly handle the data being exchanged. Some other internal assessments can be performed by a system watchdog which can assess the state of applications. External assessments must be performed by separate systems, such as gateways, proxy servers, and routers.

This monitoring is for the data exchanges and other end system processes beyond the communications network and the protocol stack, since those are handled by the communication network NSM objects. Since these end systems can be very different in their applications and in their validity checking of the data exchanges, the actual meaning or causes of “invalid data” must be considered a local issue.

The following is a list of monitored data from end systems:

- invalid data detected by end device application;
- invalid requests for data detected by end device application;
- invalid control commands detected by end device application;
- status of each application and/or software module: stopped, suspended, running, not responding, inadequate or inconsistent input, errors in outputs, error state, etc.;
- status of all network connections to an end device, including availability, overloads;
- status of any “keep-alive” heartbeats, including any missed heartbeats;
- status of backup or failover mechanisms, such as numbers and times these mechanisms were unavailable;

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

- status of data reporting: normal, not able to keep up with requests, missing data, etc.;
- status of access: numbers, times, and types of unauthorized attempts to access data or issue controls;
- anomalies in data access (e.g. individual request when normally reported periodically);
- numbers and times of all stops and starts of systems, controllers, and applications;
- log of all events, including type of event, timestamp, relevant status or situation, equipment or message identification, etc.;
- return-to-normal indications after all failures, stops, unavailability, etc.

6.2.2 Security control and management of end systems

Security management of end systems is crucial to the overall security of power system operations. This security management must be able to undertake more than just monitoring, but must also be able to control the end system, including shutting it down, restarting applications, and managing security keys and certificates:

The following is a list of security control and management commands:

- shut down end system;
- restart end system;
- start or stop reporting;
- kill and/or restart application;
- change mode of end system, such as automatic, manual, backup, off-line, etc.;
- re-establish connection to another end system;
- shut down another end system;
- provide event log of information events;
- update password;
- update security key or certificate;
- update list of authorized users;
- update list of revoked users;
- update backup or failover options;
- requesting audit logs and records.

6.3 NSM requirements: Intrusion detection functions

6.3.1 Detecting unauthorized access

The most basic intrusion detection requirement is to determine if an unauthorized entity is trying to access the system. This requirement thus relies on establishing which entities are authorized, and thereby indicating which entities are not authorized.

The NSM data objects required to detect unauthorized access include:

- determination that unauthorized user is attempting a connection or transmission of a message, based on a list of authorized users of the connections;
- identity of unauthorized user;
- updating of list of authorized users with newly authorized users and revoked users (may be done outside NSM data object process).

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

6.3.2 Detecting resource exhaustion as a denial of service (DoS) attack

Typically, the passive IDS can detect resource flooding based upon time and/or bandwidth consumption (e.g. similar to a SYN flood attack). This works well for resource "unconstrained" devices, but not well within the TC 57 domain where communication resources are limited. The reasons are as follows.

a) In typical networks, an IDS may be able to detect a SYN flood attack where hundreds or thousands of rapid SYNs are issued (e.g. an attack designed to consume available TCP connections). However, in TC 57 domain networks, IEC 60870-5-104, IEC 60870-6, and IEC 61850 devices do not support hundreds or thousands of connections (e.g. probably less than 16 in a control centre to substation environment).

b) Due to the lower number of possible connections, the timeframe required for the equivalent of the SYN flood attack has to be shorter, and probably most passive IDSs would not be able to detect such an attack. A possible solution could be to configure these passive IDSs based on the expected resource capacity, but this complicates configuration and maintenance of the communication networks, since each time they are reconfigured, the IDSs would also have to be updated.

c) An alternative solution is to let the network itself dynamically reconfigure what might constitute an SYN flood attack. The COMM stack and applications do have an explicit knowledge of the resources, and this explicit knowledge of resources can be accessed through standardized NSM data objects.

The NSM data objects required to detect resource exhaustion attacks include:

- exceeding the maximum number of connections permitted over the network;
- count of number of connections actually in place over the network;
- exceeding the maximum number of connections which can be in use simultaneously;
- count of the number of connections in use simultaneously;
- exceeding minimum/maximum idle time (to detect hung connections);
- actual idle time over a specified time period;
- exceeding CPU load limits;
- exceeding memory usage limits;
- below low level battery power limits or too high rate of change.

This information must be collected from each "node" along the entire communication path between applications, since different communication segments between nodes could be affected and cause a bottleneck.

6.3.3 Detecting buffer overflow DoS attacks

Passive IDSs are not intrinsically able to determine whether a buffer overflow attack is underway. This is especially true for IEC 61850 and IEC 60870-6 TASE.2, where the application buffer size is negotiated at runtime. However, the application/communication stack might be aware of such overruns. This even applies to Ethernet buffer issues internal to the communication stacks.

The NSM data objects required to detect buffer overflow attacks include:

- number of buffer overruns;
- number of buffer under runs;
- audit ability to detect which source caused the buffer overflow/underflow.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

6.3.4 Detecting tampered/Malformed PDUs

Passive IDSs can have an ability to detect some malformed packets. However, it is almost impossible for passive IDSs to detect a packet that has been tampered with (e.g. man-in-the-middle). Additionally, for more complex application level protocols (e.g. IEC 60870-5, IEC 61850, and IEC 60870-6 TASE.2), passive IDSs may not have the ability to detect all of the possible malformations that could cause processing issues. However, the communication stack, application, and/or IS does have this knowledge, since they must interpret each packet.

The NSM data objects in this category include:

- number of malformed PDUs detected;
- number of PDUs which have been tampered with;
- audit ability to detect which source is causing the tampered/malformed PDU.

6.3.5 Detecting physical access disruption

If a resource is powered-off or disconnected from the communication network, this represents the ultimate DoS attack, since physical restoration may be required. Especially if the equipment cannot be turned back on remotely, it is vital to be able to accurately log the time of the power-off/disconnect event and to correlate it with other events.

The NSM data objects required to detect physical access disruptions include:

- loss of power to equipment and time of loss;
- media disconnected and time of disconnect;
- power restored to equipment and time of restoration;
- media re-connected and time of reconnection.

6.3.6 Detecting invalid network access

Firewalls 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. Other firewall capabilities include port restrictions, stateful filtering and session management.

However, internal (e.g. behind a firewall) resources can be converted into (inadvertent or deliberate) attackers. In many situations, this type of “conversion” is detectable by passive IDSs. However, IDSs within a network may not be able to recognize invalid data exchanges which take place. For example, any protocols used both internally and externally, such as IEC 60870-6 (TASE.2) and now IEC 61850 between substations and control centres, could pass malicious data from an external source (which is trusted only for certain types of data) to an internal resource, where it might be sent as fully trusted data to other internal resources.

Much of the protection for this type of attack would have to be within the actual applications which handle the exchange of data between external resources and internal resources. These applications should have the knowledge of what data is valid and/or not valid. However, some NSM data objects that monitor the traffic between applications/systems could assist in this effort.

The NSM data objects required to help detect invalid network access include:

- unexpected frequency of traffic between specific applications/systems on the network;
- unexpected volume of traffic between specific applications/systems on the network;
- suspicious data detected (virus, worm, or malformed data).

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

6.3.7 Detecting coordinated attacks

Coordinated attacks across many substations, control centres and utilities could inflict more damage than these same attacks might cause if they were executed at different times or places. If sequential attacks are underway, then it could be vital to respond appropriately and in a timely manner to the first attacks to mitigate the impact of the remaining attacks.

Whether or not specific attacks are successful, the knowledge that they were coordinated can provide significant clues on who caused them, how they were executed, and why they took place.

Therefore, a mechanism for the correlation of information needs to be standardized. Conceptually, this mechanism is simple: a complete log of all significant alarms and events (including events that should have taken place and did not occur or failed) with synchronized and precise timestamps.

In practice, the precision, time zone, and accuracy of timestamps have varied significantly. Therefore, timestamp standards should use ISO 8601 time format, with the ability to record up to millisecond precision, and with adequately accurate time synchronization across systems. This time synchronization could be within 1 ms for some functions, but should at least be within a few seconds for most other functions.

The NSM data objects required to help detect coordinated attacks include:

- identification of all communication failures;
- identification of all end-system failures;
- identification of all DoS attacks;
- timestamps with millisecond precision on all data objects;
- time synchronization within directly interconnected systems within at least one second;
- time synchronization across all communications and end systems within at least a few seconds.

7 NSM abstract data types

7.1 Abbreviated terms

IEC 61850-7-4, Clause 4, defines abbreviated terms for building concatenated data names. The following abbreviated terms are used as additional terms for building concatenated Data Names. IEC 61850-7-4 and IEC 61850-7-420 terms are used where these exist.

Term	Description
ACL	Access control list
App	Application or software module
Atk	Attack
Auth	Authorized
Avail	Available
Buf	Buffer
Byt	Byte
Cert	Certificate
Conn	Connection

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Term	Description
Dct	Detection
End	End system, e.g. IED, RTU, gateway
Exh	Exhaustion
Fail	Failure
Frq	Frequency of events
Hrd	Hardware
Lnk	Link
Mal	Malformed
Msg	Message
Net	Network
Nod	Node in network
Pass	Password
Pdu	Protocol data unit (PDU)
Prot	Protocol
Pth	Path or communications link
Resc	Resource
Rout	Router, bridge, or gateway in network
Rtry	Retry
Sim	Simultaneous
Tamp	Tampered with
Trf	Traffic
UnAuth	Unauthorized
Usr	User

7.2 NSM data object constructs

7.2.1 NSM data object fields

The types of NSM data object fields are listed below.

- Group: This is the group (e.g. equipment, system, or set of applications) of which the data object is a member.
- Name: This is a unique alphanumeric name within the context of the data group. It is constructed from well-defined terms and from other appropriate letters and numbers.
- Description: This is a free text description of the data object.
- Simple data types: This denotes the type of the object as using one of the following basic formats:
  - binary;
  - integer;
  - floating point;

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

  - text (visible string);
  - resource identifier (master resource identity – mrID or object identifier – OID);
  - IP address;
  - counter;
  - date;
  - time ticks;
  - time (elapsed time, time of day, etc.);
  - array.
- High level data types: This denotes the type of the object as using one of the following more complex data types:
  - alarm (binary alarm state);
  - status (binary, integer, counter, or enumeration states);
  - measurement (integer, counter, enumeration, or floating point of externally measured value);
  - setting (integer, enumeration, or floating point used to establish a value for use by end system);
  - OI array (array of object Identifier elements);
  - VS array (array of visible string elements);
  - Int array (array of integer elements);
  - FP array (array of floating point elements);
  - table (two or more columns and/or rows);
  - control hardware (binary control command for triggering an action);
  - control software (application call to software optionally containing parameters);
  - opaque (not known / not specified / special).
- Access: This designates the access permissions for the object and can be one of the following:
  - read-only (r-o);
  - read-write (r-w);
  - write-only (w-o).
- Mandatory/optional: This designates the requirement for the object and can be one of the following:
  - mandatory (M);
  - optional (O);
  - conditional (C);
  - deprecated / obsolete (D).

7.2.2 Construction of data objects

Each data object will consist of the following parts.

- Resource identity: The name or identity of the resource (equipment, communications channel, or system) associated with the data object. This resource identity is implementation-dependent and may be a “master resource Id” (MRID) or “object identifier” (OID).
- Data object name or identity: The name or other identity of the data object.
- Data type: The data type will indicate the type of value of the data object.
- Quality: The quality or validity of the data value, indicating at a minimum “normal/good”, “questionable”, and “invalid”.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

- Timestamp: The time and date when the value or quality was last updated.
- Change indication: which item changed: value or quality (optional).
- Description (optional).
- Additional fields (optional).

7.2.3 Access to data objects

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.

These access permissions shall be coordinated with role-based access control (IEC/TS 62351-8)[1].

7.3 High level NSM data type structures

The following high level NSM data type structures are described using XML schema definition (XSD) diagrams strictly as a method for defining the structures – the mapping of these data types to protocols may or may not use XSD.

Figure 6 defines alarm objects.

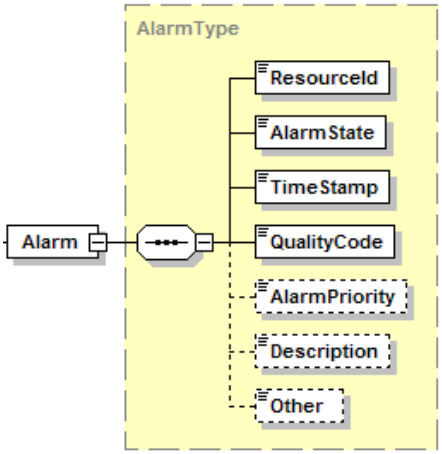

Figure 6 – Alarm structure

[1] Under consideration.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Figure 7 defines status data objects.

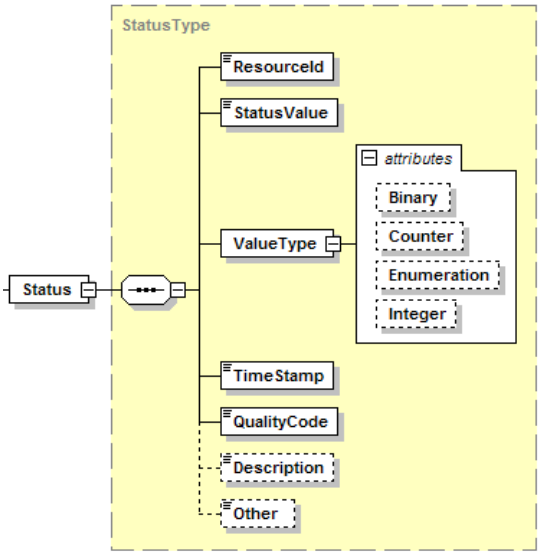

Figure 7 – Status structure

Figure 8 defines measurement data objects.

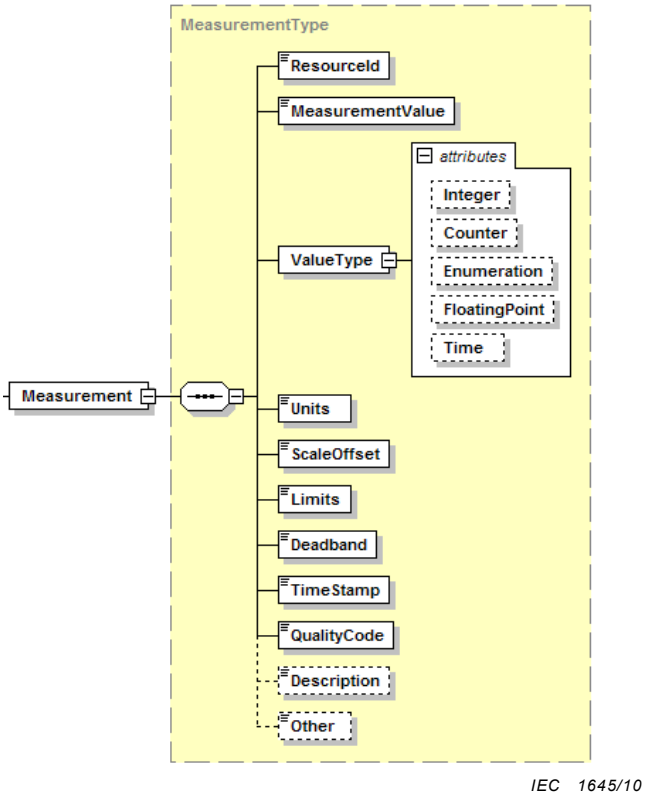

Figure 8 – Measurement structure

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Figure 9 defines setting data objects.

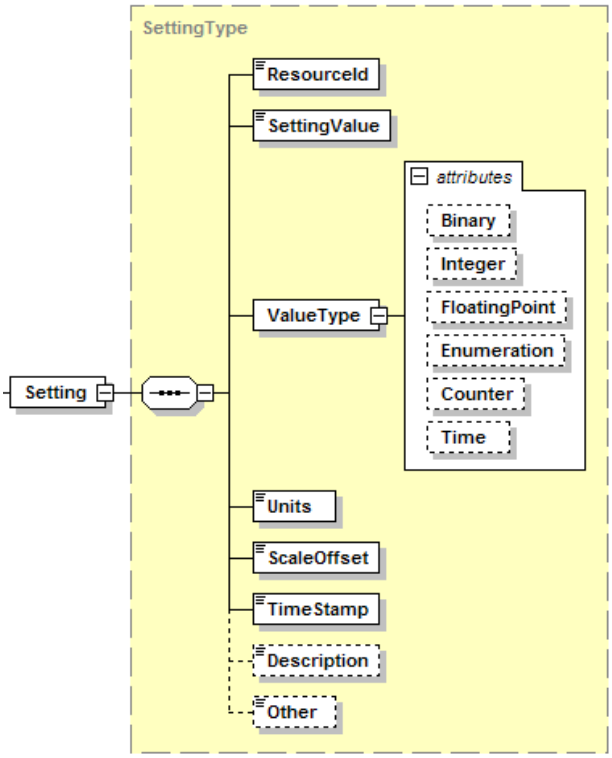

Figure 9 – Setting structure

Figure 10 defines array data objects, including OI array, Int array, VS array, and FP array.

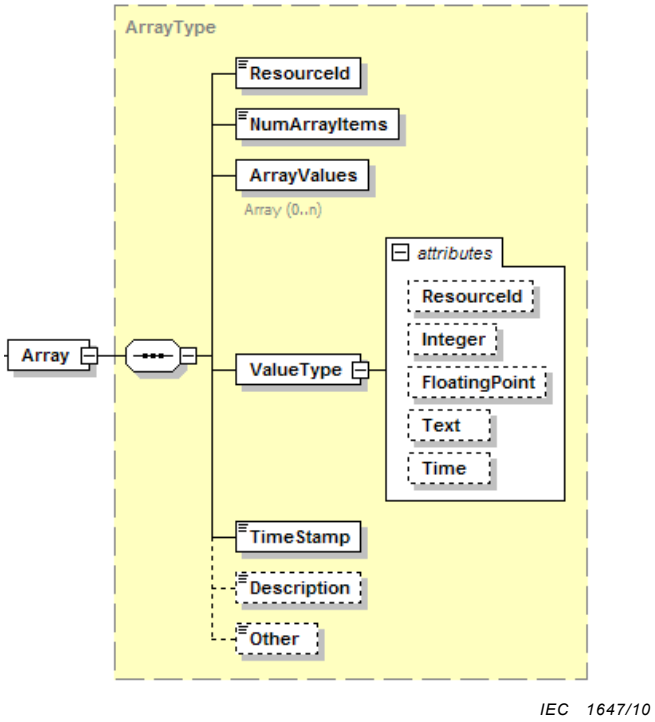

Figure 10 – Array

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Figure 11 defines table data objects.

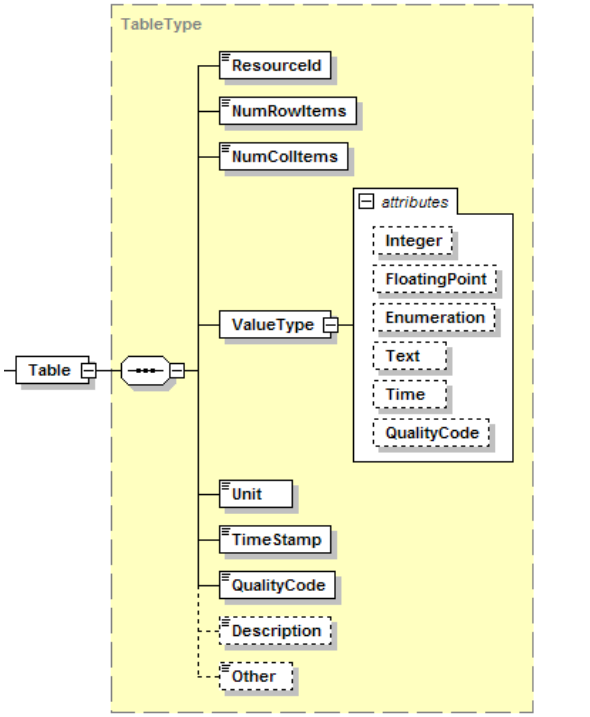

Figure 11 – Table

Figure 12 defines control hardware data objects, which consist of a binary control command for triggering actions.

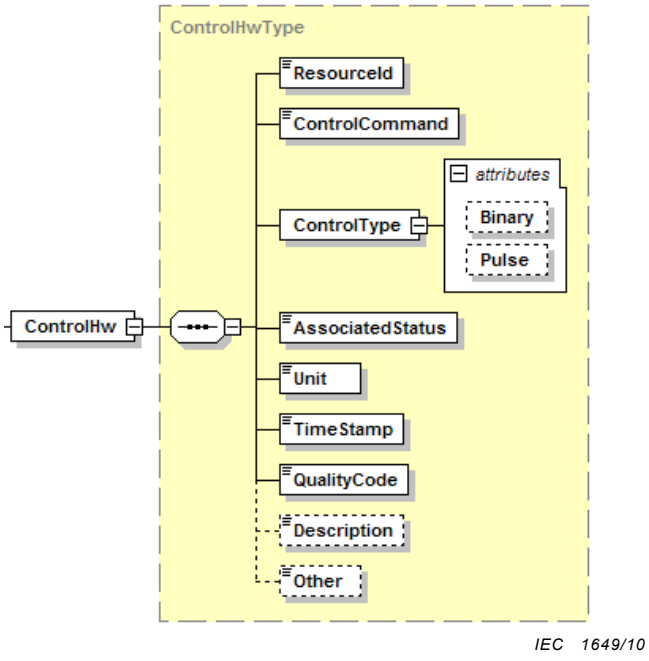

Figure 12 – Control hardware

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Figure 13 defines control software data objects, which consist of application calls to software and optionally contains parameters.

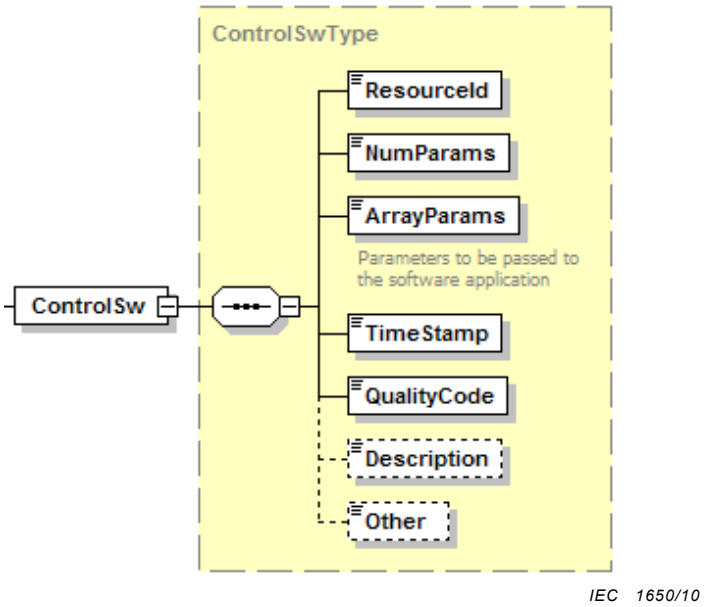

Figure 13 – Control software

7.3.1 Opaque (not known / not specified / special)

This data object has no standardized structure.

8 NSM abstract data objects

8.1 Communications health NSM data objects

8.1.1 Network configuration monitoring and control

As discussed in 6.1.1, the following NSM data objects are used for network configuration monitoring and control.

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.

Object	Data type	Definition	Access	M/O
Configuration settings				
EndLst	OI Array	List of end systems connected in network	r-w	O
NodLst	OI Array	List of intermediate network nodes, such as routers, bridges, gateways, etc.	r-w	O
PthLst	OI Array	List of paths in network	r-w	O
ACLLst	OI Array	Set or update the access control list, based on the list of object identifiers	r-w	O
PthRoutLst	OI Array	List of path routes and routing priorities to end devices	r-w	O
ActSet	VS Array	Set action steps for equipment failures, such as switch to backup	r-w	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Object	Data type	Definition	Access	M/O
Status				
EndDct	Status	Detection of connect or disconnect of an end device in the network	r-o	O
NodDct	Status	Detection of a new network node	r-o	O
PthDct	Status	Detection of a new path	r-o	O
Setpoint				
NodSet	Setting	Set parameter of a node	r-o	O
Controls				
HrdPwr	Control Hardware	Switch power on or off of a specified piece of hardware – hard disconnect from power	w-o	O
NodRs	Control Software	Reset node through software capabilities	w-o	O

8.1.2 Network backup monitoring

As discussed in 6.1.2, the following NSM data objects are used for monitoring the backup and failover state of the network.

Object	Data type	Definition	Access	M/O
Configuration settings				
NetAltPth	OI Array	List of alternate or backup paths for each primary path in the network	r-w	O
NetAltNod	OI Array	List of alternate or backup network equipment for each primary equipment	r-w	O
Alarms				
AltPthLos	Alarm	Required number of alternate or backup paths has been lost	r-o	O
AltPthSw	Alarm	Uncommanded switch to alternate or backup path has taken place	r-o	O
AltNodLos	Alarm	Required number of alternate or backup equipment has been lost	r-o	O
AltNodSw	Alarm	Uncommanded switch to alternate or backup equipment has taken place	r-o	O
Values				
AltPthSt	Status	Status of alternate paths	r-o	O
AltNodSt	Status	Status of network equipment	r-o	O
Log				
PthLog	Log	Log of all path configuration changes	r-o	O
NodLog	Log	Log of all equipment status changes	r-o	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

8.1.3 Network communications failures and degradation monitoring

As discussed in 6.1.2, the following NSM data objects are used for network failure monitoring. These can be used on a per physical link basis or at any network level. If routers, bridges, hubs, and other networking equipment support SNMP MIBs, these NSM data objects may supplement or be integrated with them.

Object	Data type	Definition	Access	M/O
Configuration settings				
ConnFailTmms	Time	Elapsed time to distinguish a permanent failure from a temporary failure	r-w	O
ConnRtryCnt	Integer	Number of retries after loss of connection to distinguish a permanent failure from a temporary failure	r-w	O
ConnRtryTmms	Time	Elapsed time between retries during temporary failure	r-w	O
ConnFailRtryCnt	Integer	Number of retries after a permanent failure	r-w	O
ConnFailRtryTmms	Time	Elapsed time between retries after permanent failure	r-w	O
Alarms				
ConnAlm	Alarm	Connection failure	r-o	O
ConnFailAlm	Alarm	Connection permanent failure	r-o	O
ConnFlovAlm	Alarm	Connection failover	r-o	O
Values				
RsTmms	Time	Total time since last reset	r-o	O
ConnFailTot	Count	Total number of failures since reset	r-o	O
ConnTotTmms	Time	Total time connected since reset	r-o	O
ConnCurTmms	Time	Elapsed time connected since last connection was established	r-o	O
ConnAvTmms	Time	Average length of time of connections	r-o	O
ConnRej	Integer	Number of rejected connections	r-o	O
ConnFlovId	ObjectId	Identity of connection failed over to	r-o	O
Controls				
ConnRs	Control	Reset number and time of connection	w-o	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

8.1.4 Communication protocol monitoring

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.

Object	Data type	Definition	Access	M/O
Configuration settings				
ProtId	ObjectId	Protocol identification	r-w	O
ProtVer	ObjectId	Protocol version	r-w	O
RescExhPct	Integer	Percentage of resource busy to cause exhaustion alarm	r-w	O
Alarms				
ProtMisAlm	Alarm	Protocol mismatch – version or access parameters	r-o	O
TimSyncAlm	Alarm	Time synchronization alarm	r-o	O
ProtMessAlm	Alarm	Protocol tampered/malformed message alarm	r-o	O
ProtAcsAlm	Alarm	Invalid protocol access alarm	r-o	O
RescExhAlm	Alarm	Resource exhaustion alarm – sent when resource is over x % busy	r-o	O
BufOvrfAlm	Alarm	Buffer overflow alarm	r-o	O
NetAcsAlm	Alarm	Invalid network access alarm	r-o	O
ObjAcsAlm	Alarm	Invalid object access alarm	r-o	O
Values				
MsgDlvTmmsAv	Time	Average message delivery time	r-o	O
MsgDlvTmmsMin	Time	Minimum message delivery time	r-o	O
MsgDlvTmmsMax	Time	Maximum message delivery time	r-o	O
MsgCnt	Counter	Count of messages	r-o	O
MsgBytAv	Integer	Average message byte size	r-o	O
MsgBytMin	Integer	Minimum message byte size	r-o	O
MsgBytMax	Integer	Maximum message byte size	r-o	O
LnkLstAuthOut	OI Array	List of authorized links from this network device	r-o	O
LnkLstAuthIn	OI Array	List of authorized links to this network device	r-o	O
LnkLstAvail	OI Array	List of available links from this network device	r-o	O
Controls				
MsgDlvTmmsRs	Control	Reset message delivery time statistics	w-o	O
MsgBytRs	Control	Reset message byte size statistics	w-o	O

8.2 End system health NSM data objects

8.2.1 End system monitoring

The following NSM data objects are used for monitoring end systems, including IEDs, RTUs, gateways, data concentrators, etc.

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Object	Data type	Definition	Access	M/O
Configuration settings				
EndOI	Object Identifier	Object identifier name of this end system	r-w	O
NetOILst	OI Array	List of network connections to end system	r-w	O
EndOILst	OI Array	List of those other end systems with authorized data exchanges	r-w	O
EndOIRole	VS Array	Roles of other end systems with respect to this system	r-w	O
Alarms				
DataInvAlm	Alarm	Invalid data	r-o	O
ReqInvAlm	Alarm	Invalid request for data	r-o	O
CntInvAlm	Alarm	Invalid control command	r-o	O
AppAlm	Alarm	Software application failure alarm	r-o	O
AppDatAlm	Alarm	Software application data alarm	r-o	O
NetAlm	Alarm	Network connection alarm	r-o	O
EndAlm	Alarm	Heartbeat failure alarm	r-o	O
EndBckAlm	Alarm	Device/system backup not available alarm	r-o	O
Values				
AppSt	OI Status	Status of an application or software module: stopped, suspended, running, not responding	r-o	O
AppStrCnt	Counter	Number of application starts or resets	r-o	O
AppDatSt	OI Status	Status of input data to an application or software module: invalid, incomplete, missing, not received in timely manner, not output in a timely manner	r-o	O
NetSt	OI Status	Status of network connections: available, not available, overload	r-o	O
EndSt	OI Status	Status of end device, including availability, heartbeat state	r-o	O
EndBckSt	OI Status	Status of any backup devices, systems, or applications, including availability	r-o	O
DatUnAuthAcsCnt	Counter	Number of unauthorized attempts to access data	r-o	O
DatMisCnt	Counter	Number of lost data events	r-o	O
EndStrCnt	Counter	Number of device/system starts or resets	r-o	O
Log				
EndLog	Log	Log of all significant events occurring in end system	r-o	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

8.2.2 End system security management

The following NSM data objects are used for the security management of end systems, including IEDs, RTUs, gateways, data concentrators, etc.

Object	Data type	Definition	Access	M/O
Controls				
EndHrdOff	Control Hardware	Power off the end system: either this one or another one	w-o	O
EndHrdOn	Control Hardware	Power on the end system	w-o	O
EndRs	Control	Reset end system	w-o	O
AppOff	Control	Kill software application	w-o	O
AppRs	Control	Reset software application	w-o	O
EndOpMod	Control	Change mode of end system: automatic, manual, backup, off-line	w-o	O
EndConnEst	Control	Establish connection with another end system	w-o	O
EndLogCtr	Control	Request log of end system	w-o	O

8.3 Intrusion detection NSM data objects

Based on role-based access control.

8.3.1 Unauthorized access NSM data objects

The following NSM data objects are used to detect attempts at unauthorized access.

Object	Data type	Definition	Access	M/O
Configuration settings				
AuthUsrLst	OI Array	List of authorized users and their privileges	r-w	O
Alarms				
UnAuthAlm	Alarm	Unauthorized user attempting connection	r-o	O
Values				
UnAuthUsrId	ObjectId	Identity of unauthorized user: IP address?	r-o	O
UnAuthUsrCnt	Integer	Number of unauthorized connection attempts	r-o	O
UnAuthRte	Integer	Rate of unauthorized connection attempts	r-o	O

8.3.2 Resource exhaustion NSM data objects

The following NSM data objects are used to detect resource exhaustion conditions.

Object	Data type	Definition	Access	M/O
Configuration settings				
ConnCnt	Counter	Count of connections permitted	r-w	O
ConnSimCnt	Counter	Count of simultaneous connections permitted	r-w	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Object	Data type	Definition	Access	M/O
Alarms				
ConnExcAlm	Alarm	Alarm on maximum number of connections exceeded	r-o	O
ConnExcSimAlm	Alarm	Alarm on maximum number of simultaneous connections exceeded	r-o	O
IdlTmmsMinAlm	Alarm	Alarm on exceeding min idle time	r-o	O
IdlTmmsMaxAlm	Alarm	Alarm on exceeding max idle time	r-o	O
Values				
ConnExcMax	Integer	Maximum number of connections exceeded	r-o	O
ConnExcSimMax	Integer	Maximum number of simultaneous connections exceeded	r-o	O
IdlTmms	Time	Actual idle time	r-o	O

8.3.3 Buffer overflow NSM data objects

The following NSM data objects are used to detect resource exhaustion conditions.

Object	Data type	Definition	Access	M/O
Alarms				
BufOvAlm	Alarm	Alarm on buffer overflow	r-o	O
BufUnAlm	Alarm	Alarm on buffer under run	r-o	O
Values				
BufOvCnt	Integer	Count of buffer overruns	r-o	O
BufUnCnt	Integer	Count of buffer under runs	r-o	O
BufUsrId	VisibleString	Identity of user causing buffer problems	r-o	O

8.3.4 Tampered/malformed PDUs

The following NSM data objects are used to detect PDUs which are malformed or tampered with.

Object	Data type	Definition	Access	M/O
Alarms				
PduMalAlm	Alarm	Alarm on malformed PDU	r-o	O
PduTampAlm	Alarm	Alarm on tampered PDU	r-o	O
Values				
PduMalCnt	Integer	Count of malformed PDUs	r-o	O
PduTampCnt	Integer	Count of tampered PDUs	r-o	O
PduUsrId	OI	Identity of user causing PDU problems	r-o	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

8.3.5 Physical access disruption

The following NSM data objects are used to detect physical access disruption.

Object	Data type	Definition	Access	M/O
Alarms				
PwrLosAlm	Alarm	Alarm on power loss	r-o	O
PwrOnAlm	Alarm	Alarm on power on	r-o	O
ComLosAlm	Alarm	Alarm on loss of communications media	r-o	O
ComOnAlm	Alarm	Alarm on communications media connection	r-o	O
DoorOpAlm	Alarm	Alarm on door open	r-o	O
SenLimAlm	Alarm	Alarm on sensor values beyond limit	r-o	O
Values				
PwrLosCnt	Integer	Count of power losses	r-o	O
ComLosCnt	Integer	Count of communication media losses	r-o	O

8.3.6 Invalid network access

The following NSM data objects are used to detect and report invalid network access.

Object	Data type	Definition	Access	M/O
Configuration settings				
TrfFrqSet	Integer	Maximum traffic frequency (PDUs per second) setting	r-w	O
TrfVolmSet	Integer	Maximum traffic volume (Bytes per second) setting	r-w	O
Alarms				
TrfFrqAlm	Alarm	Alarm on exceeding traffic frequency setting	r-o	O
TrfVolmAlm	Alarm	Alarm on exceeding traffic volume setting	r-o	O
Values				
TrfFrq	Integer	Traffic frequency	r-o	O
TrfVolm	Integer	Traffic volume	r-o	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

8.3.7 Coordinated attacks

The following NSM data objects are used to detect coordinated attacks.

Object	Data type	Definition	Access	M/O
Configuration settings				
SynTmms	Time	Required system synchronization precision	r-w	O
AtkTmms	Time	Time period considered to be coordinated	r-w	O
AtkCnt	Integer	Number of attacks considered to be coordinated	r-w	O
Alarms				
SynAlm	Alarm	Alarm indicating synchronization is not within required precision	r-o	O
AtkAlm	Alarm	Alarm indicating coordinated attacks	r-o	O
Values				
SynId	ObjectId	Id of system not within time synchronization precision	r-o	O
AtkTyp	VisibleString	Attack type	r-o	O

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Bibliography

IEC 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*

IEC 60870-5-101, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

IEC 60870-5-102, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems*

IEC 60870-5-103, *Telecontrol equipment and systems – Part 5-103: Transmission protocols – Companion standard for the informative interface of protection equipment*

IEC 60870-5-104: *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

IEC 60870-6 (all parts) *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations*

IEC 61850 (all parts), *Communication networks and systems for power utility automation*

IEC 61850-7-1, *Communication networks and systems for power utility automation – Part 7-1: Basic communication structure – Principles and models*

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-7-4:2010, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-7-420, *Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources logical nodes*

IEC 61850-8-1, *Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-2, *Communication networks and systems for power utility automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC 61968 (all parts), *Application integration at electric utilities – System interfaces for distribution management*

IEC 61970, *Energy management system application program interface (EMS-API)*

IEC/TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC/TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

ISO/IEC 18043, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems*

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO CMIP: Common Management Information Protocol

IETF SNMPv2: RFC 1441, RFC 1452: Simple Network Management Protocol, version 2

IETF SNMPv3: RFC 3411, RFC 3418: Simple Network Management Protocol, version 3

_____

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when print

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch

Copyrighted material licensed to BR Demo by Thomson Reuters (Scientific), Inc., subscriptions.techstreet.com, downloaded on Nov-28-2014 by James Madison. No further reproduction or distribution is permitted. Uncontrolled when printe