

DIN EN 62351-7

ICS 33.200; 35.040

Einsprüche bis 2016-02-18

Entwurf

**Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen –
Daten- und Kommunikationssicherheit –
Teil 7: Netzwerk und System-Management (NSM) Daten-Objekt-Modelle (IEC 57/1542/CD:2015);
Text in Englisch**

Power systems management and associated information exchange –
Data and communications security –
Part 7: Network and system management (NSM) data object models
(IEC 57/1542/CD:2015);
Text in English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-12-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 218 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die englische Originalfassung des internationalen Dokuments IEC 57/1542/CD:2015 „Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden.

Das internationale Dokument wurde vom TC 57 „Power systems management and associated information exchange“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für den vorliegenden Normentwurf erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die englische Fassung der EN 62351-7 veröffentlicht. Zu deren Abschnitt 1 sowie Abschnitt 3, der die Begriffe festlegt und 5.1 bis 5.8 wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für viele der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

1 Anwendungsbereich

Diese Internationale Norm definiert Datenobjektmodelle für Netzwerk- und Systemmanagement (NSM), welche spezifisch für Betriebsabläufe von Systemen der Energietechnik sind. Die NSM-Datenobjekte werden für die Überwachung des Befindens von Netzwerken und Systemen verwendet, um mögliche Störungen der Sicherheit zu erkennen und das Betriebsverhalten und die Zuverlässigkeit der Informationsinfrastruktur zu steuern. Das Ziel ist die Festlegung einer Reihe von Abstrakten Objekten, welche die Fernüberwachung des Befindens und des Zustands von IED-, RTU-, DER-Systemen und anderen Systemen ermöglichen, die für Betriebsabläufe des Systems der Energietechnik wichtig sind.

Der Betrieb von Systemen der Energietechnik ist zunehmend abhängig von Informationsinfrastrukturen, einschließlich Kommunikationsnetzwerken, intelligenten elektronischen Geräten (IED; en: intelligent electronic devices) und selbstdefinierenden Kommunikationsprotokollen. Deshalb ist die Verwaltung von Informationsinfrastrukturen zu einer entscheidenden Frage für die Bereitstellung des erforderlichen hohen Sicherheitsniveaus und der Zuverlässigkeit des Betriebs von Systemen der Energietechnik geworden.

Die Telekommunikations-Infrastruktur, welche für die Übermittlung des Protokolls für Fernwirken und Automatisierung verwendet wird, unterliegt bereits der Steuerung der Überwachung von Befinden und Zustand, wobei das Konzept verwendet wird, welches in den Normen der IETF zum einfachen Protokoll für Netzwerkmanagement (SNMP; en: Simple Network Management Protocol) für das Netzwerkmanagement entwickelt wurde; wobei die spezifischen Geräte des Systems für Energietechnik (wie z. B. Fernschutz, Fernwirken, Stationsautomatisierung, Zeiger (en: Synchrophasor), Wechselrichter und Schutzeinrichtungen) stattdessen eine spezifische Lösung für ihre Überwachung erfordern.

Diese Objekte liefern Überwachungsdaten bezüglich TC57-Protokollen, welche innerhalb von Systemen der Energietechnik betrieben werden (IEC 61850, IEC 60870-5-104) und des gerätespezifischen Umgebungs- und Sicherheitszustands. In die Liste der überwachten Protokolle ist auch IEEE 1815 DNP3 eingeschlossen. Die NSM-Datenobjekte verwenden die in IEC 61850 entwickelten Benennungskonventionen, welche zur Behandlung von Fragen des NSM erweitert wurden. Für Zwecke der Verallgemeinerung werden diese Datenobjekte, und die Datentypen, aus welchen sie bestehen, als ein abstraktes Modell von Datenobjekten definiert.

Um die Integration der Geräte eines Systems der Energietechnik innerhalb der NSM-Umgebung zu ermöglichen, wird in dieser Norm eine Zuordnung von Objekten zu einem SNMP-Protokoll bereitgestellt.

Diese Objekte, welche bereits durch bestehende MIB abgedeckt sind, werden hier nicht definiert, aber es wird gefordert, dass sie mit bestehenden Normen übereinstimmen.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 62351-2 und die folgenden Begriffe.

Begriff	Definition
Einheitliche Modellierungssprache (en: Unified Modelling Language)	Formal und umfassend beschreibende Sprache mit Diagrammtechniken, die zur Darstellung von Software-Systemen von der Anforderungsanalyse über Auslegung und Implementierung bis zur Dokumentation verwendet wird.
Struktur von Managementinformationen (en: Structure of Management Information)	Eine angepasste Teilmenge der Abstract Syntax Notation One ASN.1 des OSI zum Schreiben von Modulen (RFC 2578) der Managementinformationsbasis (MIB). Die Struktur von Managementinformationen (SMIv2) definiert grundlegende Datentypen, ein Objektmodell und die Regeln für das Schreiben und Überarbeiten von MIB-Modulen (RFC 3410).

Begriff	Definition
Modell der Transportsicherheit (en: Transport Security Model)	Ein Modell der Transportsicherheit für das einfache Protokoll für Netzwerkmanagement zur Verwendung mit sicheren Transportmodellen im Transport-Teilsystem (RFC 5590)
Sicherheit für Datagramm der Transportschicht (en: Datagram Transport Layer Security)	Ein Protokoll, welches einen Kommunikations-Datenschutz für ein Datagramm-Protokoll bereitstellt. Das Protokoll ermöglicht es Client/Server-Anwendungen in einer Weise zu kommunizieren, dass Abhören, Manipulation oder Nachrichtenfälschung verhindert werden. Das DTLS-Protokoll basiert auf dem Protokoll der Transportschicht-Sicherheit (TLS) und stellt gleichwertige Sicherheitsgarantien (RFC 6347) bereit.

5 Einführung zu Netzwerk- und Systemmanagement (NSM) (informativ)

5.1 Ziele

Die Informationsinfrastruktur bei Betriebsabläufen der Energieversorgung besteht nicht nur aus dem Kommunikationsnetzen, sondern auch aus den zwischen Systemen ausgetauschten Daten, welche in Datenbanken gespeichert werden und durch Anwendungen in Abläufen von Systemen der Energietechnik verwendet werden. Diese Informationsinfrastruktur wird üblicherweise nicht als eine kohärente Infrastruktur behandelt, sondern wird als eine ungleiche Sammlung von Kommunikationskanälen, Gruppe unterschiedlicher Netzwerkabschnitte, verschiedenen Geräten, mehreren Datenbanken und unterschiedlichen Protokollen betrachtet. Häufig führen SCADA-Systeme einige Kommunikationsüberwachungen durch, wie z. B. ob Verbindungen zu ihren fernen Endeinrichtungen (RTU; en: remote terminal unit) verfügbar sind, und ob sie das Ereignis als verloren gegangene Verbindung markieren, wenn die Verbindung fehlschlägt. Ein Echtzeit kohärenter, vollständiger und homogener Zustand des Befindens der gesamten Informationsinfrastruktur war jedoch nicht verfügbar. Ein solcher Echtzeit kohärenter Zustand des Befindens der Informationsinfrastruktur kann Betreiber beim Erkennen und Abschwächen potentieller Probleme im System der Energietechnik unterstützen.

Bisher wurde die Informationsinfrastruktur, welche das System der Energietechnik unterstützt, nicht angemessen überwacht und einige korrigierende Bedienaktionen sind nicht möglich. Die Analyse von großen Stromausfällen in der Vergangenheit zeigte, dass die Hauptursache für die Ausweitung solcher Stromausfälle nach einem ursprünglichen Geräteausfall auf einen Mangel an der Verfügbarkeit von wesentlichen Informationen für den richtigen Nutzer zur richtigen Zeit zurückzuführen ist.

Im Fall eines Ausfalls eines Kommunikationsnetzes oder eines Systems, eines möglichen Angriffs auf die Cybersicherheit oder anderer nicht bestimmungsgemäßer Situationen muss Instandhaltungspersonal dazu in der Lage sein, die Ursache des Problems schnell zu erkennen und zu diagnostizieren: welche Einrichtung betroffen ist, wo die Einrichtung angeordnet ist und was zur Behebung des Problems unternommen werden sollte. Betreiber von Energieversorgungseinrichtungen sollten über solche nicht bestimmungsgemäßen Ereignisse schnell in der Informationsinfrastruktur informiert werden.

Verschiedene Organisationen und Versorgungsunternehmen haben unterschiedliche Bedürfnisse in Bezug darauf, welche Informationen für ihr Informationsnetzwerk wichtig sind und welche Daten für ihr Service- und Instandhaltungspersonal verfügbar sein sollten. So sind zum Beispiel Telekommunikationstechniker im Allgemeinen dafür verantwortlich, Probleme mit Mikrowellenkabeln und Lichtwellenleitern aufzuspüren; Anbieter von Telekommunikationsdiensten müssen ihre Netzwerke überprüfen; Administratoren von Datenbanken müssen ermitteln, ob Daten ordnungsgemäß von Datenbanken von Stationsautomatisierungssystemen oder von geographischen Informationssystemen (GIS) abgerufen werden; Protokolltechniker müssen Konfigurationsfehler korrigieren; Anwendungstechniker müssen bestimmen, ob Anwendungen abgestürzt sind, sich nicht angenähert haben, oder sich in einer Endlosschleife befinden; Personal der Cybersicherheit muss Kenntnis bezüglich des Ortes und der Art eines Cyberangriffs haben, welcher das Netzwerk beeinflusst; und Betreiber müssen große Datenmengen filtern, um festzustellen, ob das Auftreten eines möglichen „Problems des Systems der Energietechnik“ bevorsteht.

Die in der vorliegenden Spezifikation definierten Datenobjekte des Netzwerk- und Systemmanagements (NSM), sind spezifisch und bedeutungsvoll für die Energiewirtschaft und liefern Informationen bezüglich des Befindens von Endgeräten. Diese NSM-Datenobjekte unterstützen die Integrität von Kommunikationsnetzen, das System, das Befinden von Netzwerk und IED, Ereignisse von Intrusions Detection Systems (IDS; de: System zum Erkennen von Eindringungen) und Firewalls und andere für die Sicherheit/das Netzwerkmanagement maßgebliche Informationen. Ein Beispiel für eine Grundarchitektur, welche eine typische SCADA-Infrastruktur eines Systems der Energietechnik mit Firewalls, System zum Erkennen von Eindringungen und Objekten der Sicherheitsüberwachung erweitert, ist in Bild 1 dargestellt.

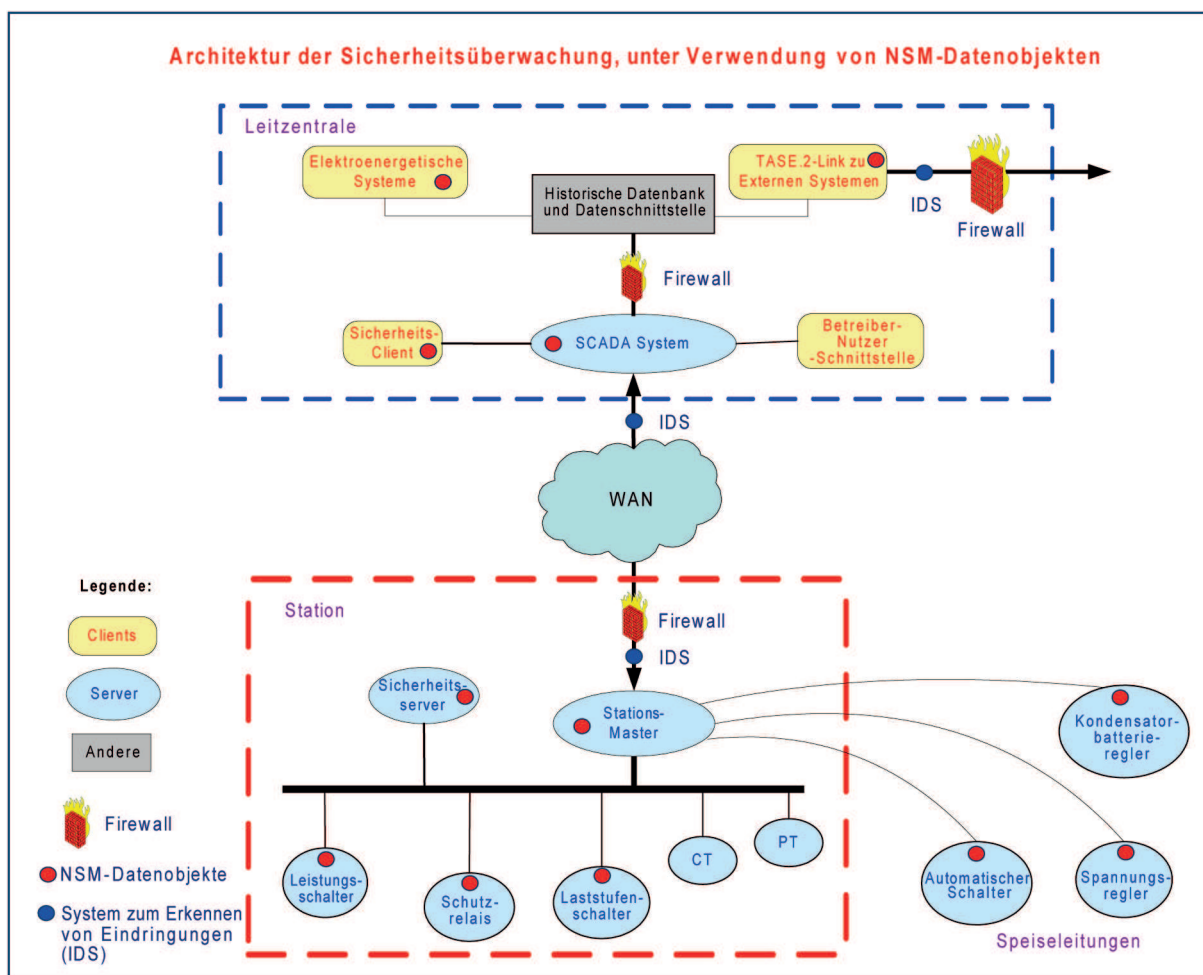


Bild 1 – Beispiel einer mit NSM-Datenobjekten erweiterten SCADA-Architektur eines Systems der Energietechnik

5.2 NSM-Konzepte

5.2.1 Einfaches Protokoll für Netzwerkmanagement (SNMP)

Das einfache Protokoll für Netzwerkmanagement (SNMP) wurde durch IETF als ein Protokoll für die Übertragung von Objekten der Managementinformationsbasis (MIB) über das Internet entwickelt. Eine Managementinformationsbasis (MIB) ist eine Datenbank, welche hierarchische Datenobjekte definiert, wobei auf jedes Objekt durch einen Objektbezeichner (OID; en: object identifier) verwiesen wird. Diese Datenobjekte werden verwendet, um zu definieren, welche Informationen zur Überwachung und Verwaltung einer Netzwerkinfrastruktur verwendet werden dürfen. MIB-Objekte sind so festgelegt, dass sie den Zustand verschiedener Einrichtungen, Anwendungen und Systeme abbilden.

Viele Systeme verwenden SNMP auch über interne Kommunikationsnetze. Aufgrund der Beliebtheit von SNMP ist SNMP das bevorzugte Protokoll für die MIB-Übertragung. Andere Protokolle dürfen jedoch ebenfalls verwendet werden.

Die IETF (Internet Engineering Task Force) und viele herkömmliche Anbieter von Netzwerk- und Systemprodukten haben spezifische MIB für ihre Produkte entwickelt, wobei die grundlegende Annahme die ist, dass diese Produkte über das Internet oder ein Intranet auf der Grundlage von IETF-Technologien verwendet werden.

Obwohl einige bestehende MIB-Objekte ausreichend allgemein für typische Netzwerkeinrichtungen sind und durch die Energiewirtschaft verwendet werden sollten, sind viele spezialisierte MIB erforderlich, um einige der sehr spezialisierten Einrichtungen und besonderer Umgebungen, welche in Betriebsabläufen von Systemen der Energietechnik verwendet werden, abzubilden.

5.2.2 ISO-NSM-Kategorien

Aspekte des Netzwerkmanagements wurden durch ISO in 5 Bereiche eingeteilt:

- Leistungsmanagement;
- Konfigurationsmanagement;
- Buchhaltungsmanagement;
- Störungsmanagement;
- Sicherheitsmanagement.

Von diesen 5 Bereichen ist Buchhaltungsmanagement für die vorliegende Norm nicht maßgeblich. Die anderen 4 Bereiche sind entweder direkt oder indirekt an der Sicherheit der Energieversorgungsabläufe beteiligt. Wenn zum Beispiel der Ausfall einer Einrichtung oder eine unachtsame Parameteränderung eine Verschlechterung des Leistungsvermögens verursacht, kann die Zuverlässigkeit der Betriebsabläufe des Systems der Energietechnik beeinträchtigt werden; oder eine Änderung der Netzwerkkonfiguration könnte eine einzelne Fehlerstelle hervorrufen, welche nicht erkannt wird, bevor dieser Fehler auftritt; oder eine nicht erkannte Eindringung kann die Verletzung von Einschränkungen der für zeitempfindliche Datenübertragungen erforderlichen Übertragungszeit hervorrufen.

5.2.3 NSM-„Datenobjekte für den Betrieb von Energiesystemen

Die in der vorliegenden Norm identifizierten NSM-„Datenobjekte“ füllen die Lücke zwischen der bestehenden SCADA-Kommunikationsüberwachung und der erwünschten sicheren und zuverlässigen Informationsinfrastruktur für die Betriebsabläufe von Energiesystemen. „Datenobjekte“ sind abstrakte Datenelemente, welche nachfolgend auf verschiedene Protokolle abgebildet werden können, einschließlich IEC 61850, IEC 60870-5, IEC 60870-6 (TASE.2) und SNMP.

Die vorliegende Norm legt auch nicht die Maßnahmen fest, welche nach dem Empfang von Alarmen oder Warnhinweisen ergriffen werden sollten: diese Maßnahmen werden als spezifisch für ein Gerät und eine Systemimplementierung betrachtet und liegen außerhalb des Anwendungsbereiches der vorliegenden Norm.

5.3 Management von Kommunikationsnetzen

5.3.1 Netzwerkkonfiguration

Typisches Netzwerkmanagement umfasst Überwachung und Steuerung des Kommunikationsnetzes und seiner Konfiguration. Die meisten Anbieter von Netzwerkeinrichtungen auf Unternehmensebene stellen einen gewissen Grad an Steuerung bereit. Wo immer diese Steuerungsfähigkeiten in Betriebsabläufen von Energiesystemen verfügbar sind, sollten diese Fähigkeiten angewendet werden. Die Folgenden sind die NSM-Anforderungen in Bezug auf Überwachung und Steuerung der Konfiguration eines Netzwerks. Konzeptionell enthält jede Instanz im Netzwerk (entweder ein „Netzwerkknoten“ oder ein „Endgerät“ oder ein verschachteltes „Teilnetz“) diese Information. In Abhängigkeit von der Implementierung und der Konfiguration kann diese Information je nachdem von einem anderen Knoten „heruntergeladen“ oder „automatisch bezogen“ werden; wobei sie zur Ansicht oder zum Hochladen, usw. verfügbar ist.

Die folgenden Punkte sind Beispiele von Daten, die für die Überwachung und Steuerung einer Netzwerkkonfiguration zu überwachen sind.

- Informationen zur Netzwerkkonfiguration, einschließlich dazu, welche Endsysteme mit welchen Netzwerkpfaden verbunden sind. Backup- und Ersatzpfade sollten ebenfalls eingeschlossen werden. Obwohl einige Implementierungen die Datenobjekte der Konfiguration vorladen könnten, sollten sie für befugte Anwender sichtbar sein.
- Energieverwaltungsbefehle (EIN/AUS) an eine Netzwerkeinrichtung.
- Rücksetzbefehl an Netzwerkeinrichtung.
- Aufbau primärer und, wahlfrei, sekundärer Pfade zu jedem Endgerät.
- Schaltbefehle an Netzwerkeinrichtungen zum Wechseln von Pfaden zu Geräten.
- Erstellen oder Aktualisieren der Zugriffssteuerungsliste und von RBAC-Regeln.
- Einstellen von Parametern und Abfolgen für automatisierte Netzwerkmaßnahmen als Antwort auf Ereignisse, wie z. B. Neukonfiguration des Kommunikationsnetzwerks nach Ausfall einer Einrichtung.
- Spezifische Zuordnungen zum Überwachungs- und Steuerungsprotokoll dürfen gegebenenfalls auf einige der vorgenannten Daten verzichten, um duplizierte und möglicherweise widersprüchliche Konfigurationen zu vermeiden.

5.3.2 Netzwerk-Backup

Zusätzlich zur Überwachung der Netzwerkgeräte ist es wichtig, zur ermitteln, ob das Netzwerk in der Lage ist, sein Leistungsvermögen bereitzustellen, für welches es ausgelegt wurde. Insbesondere der Status von Ersatzpfaden und Backup-Geräten bedarf der Überwachung, um sicherzustellen, dass sie für den Umgang mit Ausfällen, beschädigten Kommunikationsverbindungen und dem vorsätzlichen Entfernen der Primär-routen für Zwecke der Instandhaltung oder andere Zwecke verfügbar sind.

Die Anforderungen an die Überwachung des Netzwerk-Backups umfassen:

- Ermitteln des Status von Backup-Einrichtungen, einschließlich der Fähigkeit automatisch darauf geschaltet zu werden;
- Ermitteln des Status von Ersatz-Kommunikationsverbindungen, einschließlich der verfügbaren Bandbreite, wenn sie auf sie geschaltet wurden;
- Erkennen der Fehlerumschaltung von einem Netzwerkgerät auf ein Backup-Gerät;
- Erkennen des Schaltens auf Ersatz- oder Backup-Kommunikationsverbindungen;
- Protokollieren von Status und Zeit aller Fehlerumschaltungen und der Anwendung von Backup-Geräten.

5.3.3 Kommunikationsausfall und -beeinträchtigung

Netzwerkmanagement umfasst die Überwachung des Zustands des Kommunikationsnetzes, vorwiegend für den Ausfall von Einrichtungen und der Kommunikation. Die meisten Einrichtungen auf Unternehmensebene von herkömmlichen Anbietern schließen bereits SNMP-MIB für die Überwachung dieser Netzwerke ein. Die meisten Kommunikationsnetze, die im Betrieb von Energiesystemen verwendet werden, verwenden diese Typen von herkömmlichen Netzwerkeinrichtungen jedoch nicht, da häufig kein „Netzwerk“ beteiligt ist – lediglich langsame Punkt-zu-Punkt-Verbindungen zwischen der Leitzentrale und jeder Station. Sogar dort, wo Netzwerke beteiligt sind, werden sie häufig eher als Gruppe fester Verbindungen behandelt denn als echte Netzwerke.

Wenn eine spezifische Implementierung ein herkömmliches Netzwerkgerät mit MIB mit SNMP umfasst, welches einige der folgenden Aspekte abdeckt, sollten diese deshalb wenn möglich angewendet werden. Für andere Implementierungen und andere Aspekte, die nicht durch MIB von herkömmlichen Anbietern abgedeckt werden, müssen Datenobjekte entwickelt werden. Diese Datenobjekte können dann dort implementiert werden, wo dies zweckmäßig ist.

Die Anforderungen an die Überwachung des Ausfalls und der Beeinträchtigung der Kommunikation umfassen:

- Erkennen von dauerhaften Ausfällen von Netzwerkgeräten;
- Erkennen von vorübergehenden Ausfällen und/oder Rücksetzungen von Netzgeräten;

- Erkennen von Ausfällen von Kommunikationsverbindungen;
- Erkennen von Beeinträchtigungen einer Kommunikationsverbindung oder einem unerwartet geringen Datendurchsatz;
- Erkennen von Beeinträchtigungen eines Netzwerk-Routings (Wegewahl) oder einem unerwartet geringen Datendurchsatz
- Protokollierung des Ausfalls von Geräten und Kommunikationsverbindungen und beeinträchtigten Zuständen.

5.4 Kommunikationsprotokolle

Die Überwachung von Kommunikationsprotokollen, welche über Netzwerke verwendet werden, ist ebenfalls wichtig. Ein Teil dieser Überwachung kann durch Router, Gateways, Firewalls und andere Systeme, welche die Protokolle durchlaufen, durchgeführt werden. Ein Teil der detaillierteren Informationen muss jedoch durch Protokollstapel (-stacks) gesammelt werden, da dort die Kenntnisse bezüglich der ordnungsgemäßen und nicht ordnungsgemäßen Protokollbildung verortet ist.

Die Anforderungen an die Überwachung eines Kommunikationsprotokolls umfassen:

- Erkennen von Version und Status eines Kommunikationsprotokolls;
- Erkennen der falschen Zuordnung von unterschiedlichen Protokollversionen und -fähigkeiten;
- Erkennen von verfälschten/fehlerhaften Protokollnachrichten;
- Erkennen von unzureichend synchronisierten Zeitgebern über Netzwerke;
- Erkennen von Formen von „Denial-of-Service“-Angriffen (DoS; de: Dienstverweigerungsangriffe) mit Ressourcenüberlastung;
- Erkennen von DoS-Angriffen mit Pufferüberlauf;
- Erkennen von Unterbrechungen des physikalischen Zugriffs, wie z. B. Verlust oder Beeinträchtigung von Verbindungsfähigkeit;
- Erkennen ungültiger Netzwerkzugriffe;
- Erkennen ungültiger Zugriffe/Betriebsabläufe von Anwendungsobjekten;
- Unterstützen einer erweiterten Fähigkeit zum Erkennen koordinierter Angriffe über mehrere Systeme;
- Sammeln statistischer Informationen von Netzgeräten;
 - Ermitteln mittlerer Nachrichten-Zustellungsdauern, langsamste, schnellste, usw.;
 - Zählen der Nachrichtenanzahl, Größe von Nachrichten;
 - Zählen der Anzahl verloren gegangener Nachrichten;
- Bereitstellen von Auditprotokollen und -aufzeichnungen;
- Erkennen von Zeitüberschreitungen von Anwendungsprotokollen;
- Erkennen ungültiger Sequenznummern von Anwendungsnachrichten.

5.5 Management von Endsystemen

Die Überwachung von Endsystemen von Energiesystemen umfasst eine Kombination interner und externer Bewertungen ihres Befindens. Interne Bewertungen können beim Erkennen von Funktionsabweichungen genauer sein, während externe Bewertungen ihren Zustand in Situationen ermitteln können, in welchen die Anwendung oder das Endsystem nicht in der Lage ist, sich selbst zu bewerten. Interne Bewertungen können mittels Anwendungen vorgenommen werden, welche die ausgetauschten Daten direkt verarbeiten. Einige andere interne Bewertungen können mittels einer Systemselbstüberwachung (Watchdog) durchgeführt werden, welche den Zustand von Anwendungen bewerten kann. Externe Bewertungen müssen mittels getrennter Systeme durchgeführt werden, wie z. B. Gateways, Proxyserver und Router.

Da die Endsysteme von Energiesystemen sich in ihren Anwendungen und ihrer Validitätsprüfung der Datenaustausche stark unterscheiden können, müssen die tatsächliche Bedeutung oder die tatsächlichen Ursachen von „ungültigen Daten“ als eine lokale Frage behandelt werden.

Die Folgende ist eine Liste von überwachten Daten von Endsystemen:

- ungültige Daten, erkannt durch Endgerätenwendung;
- ungültiges Abrufen von Daten, erkannt durch Endgerätenwendung;
- ungültige Steuerbefehle, erkannt durch Endgerätenwendung;
- Status jeder Anwendung und/oder jedes Softwaremoduls: angehalten, ausgesetzt, laufend, antwortet nicht, unzureichender oder widersprüchlicher Input, Fehler in Outputs, Fehlerzustand, usw.;
- Status aller Netzwerkverbindungen zu einem Endgerät, einschließlich Verfügbarkeit, Überlastungen;
- Status jeglicher „Keep-Alive“-Herzschläge (Kontrollsignale zur Aufrechterhaltung), einschließlich jeglicher ausgefallener Herzschläge;
- Status von Backup- oder Fehlerumschaltungsmechanismen, wie z. B. Anzahlen und Zeiten der Nichtverfügbarkeit dieser Mechanismen;
- Status der Datenübermittlung: normal, kann nicht mit Abfrage Schritt halten, fehlende Daten, usw.;
- Status des Zugriffs: Anzahl, Zeiten und Arten des unbefugten Versuchs eines Zugriffs auf Daten oder Ausgabe von Steuerungen;
- Funktionsabweichungen im Datenzugriff (z. B. einzelne Abfragen, wenn üblicherweise periodisch übermittelt wird);
- Anzahl und Zeiten aller Stopps und Starts von Systemen, Steuerungen und Anwendungen;
- Protokoll aller Ereignisse, einschließlich Art des Ereignisses, Zeitstempel, maßgebliche(r) Status oder Situation, Identifizierung von Gerät oder Nachricht, usw.;
- Rückkehr-zu-Normal-Anzeigen nach allen Ausfällen, Stopps, Nichtverfügbarkeit, usw.

5.6 System zum Erkennen von Eindringungen (IDS)

5.6.1 IDS-Richtlinien

Systeme zum Erkennen von Eindringungen überwachen Pakete der Netzwerkkommunikation und erkennen ein jegliches Paket, welches in einem bestimmten Netzwerk fremd ist. IDS sollten Betreiber so schnell wie möglich warnen, wenn eine Eindringung erkannt wurde und sollten darüber informieren, welche Art von Schwachstelle ausgenutzt wurde.

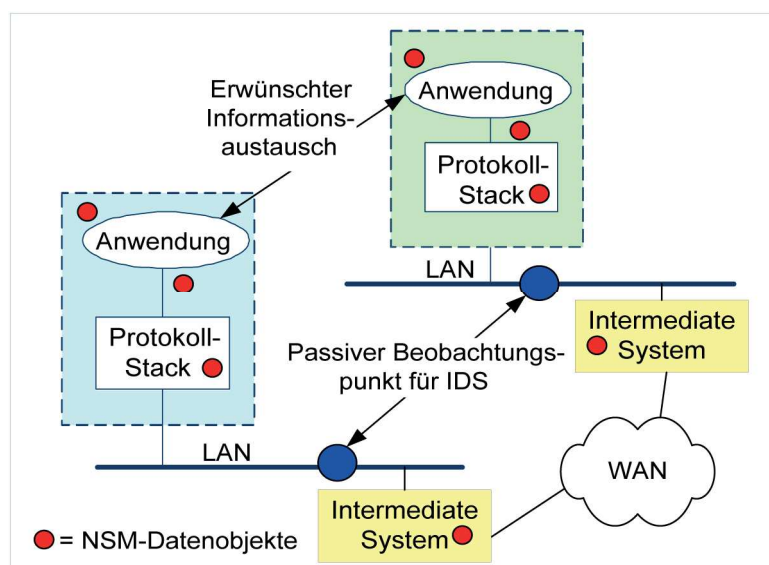


**Bild 2 – IDS-Informationsaustausch zwischen Anwendungen:
Allgemeine Kommunikationstopologie**

Dieses vereinfachte Schema zeigt zwei Anwendungen, die versuchen Informationen auszutauschen. In diesem Schema muss die Information zum Zweck des Informationsaustauschs:

- durch einen lokalen Kommunikationsstapel übermittelt werden;
- vom dem lokalen Kommunikationsstapel an ein lokales Netzwerk (LAN) übermittelt werden;
- über ein vermittelndes System (IS; en: Intermediate System) an ein Weitverkehrsnetz (WAN) geroutet/gebrückt werden;
- durch ein Remote-IS (entferntes IS) empfangen werden;
- durch ein Remote-IS an das LAN der Remote-Anwendung übermittelt werden;
- durch den Kommunikationsstapel der Remote-Anwendung empfangen werden;
- zur Verarbeitung an die Remote-Anwendung geliefert werden.

Jede dieser Stellen könnte Informationen bezüglich möglicher Erkennung von Eindringungen bereitstellen, einschließlich der folgenden Typen von Sicherheitsbedrohungen für Integrität, Vertraulichkeit, Verfügbarkeit und Unleugbarkeit:

- Ressourcenüberlastung oder „erhebliche“ Auswirkungen auf das Leistungsvermögen aufgrund einer unerwartet großen Anzahl von gesendeten Nachrichten, versehentlich oder vorsätzlich, welche den Empfang berechtigter Nachrichten verhindern oder verzögern;
- Pufferüberlauf, verursacht entweder durch „Fehler“ bei der Bildung von Nachrichten oder durch bösartige Angriffe zur Störung von Betriebsabläufen des Systems;
- PDU (Pakete), welche (versehentlich) fehlerhaft erzeugt oder (vorsätzlich) verfälscht wurden;
- ungültige Versuche eines Netzwerkzugriffs durch Nachrichten mit nicht autorisierten IP-Adressen oder Port-Anforderungen;
- ungültige Versuche eines Anwendungszugriffs.

Es gibt zwei grundlegende Methoden für IDS: passive Beobachtungstechniken und aktive Sicherheitsüberwachung. Diese werden in den folgenden Abschnitten erläutert.

5.6.2 IDS: Passive Beobachtungstechniken

Passive Beobachtungstechniken (d. h. sie erfordern keine Änderungen des IS, des COMM-Stapels oder der Anwendung) erfordern lediglich das Hinzufügen von „netzwerkbasierten IDS“-Monitoren – bestehende Einrichtungen und Netzwerke müssen nicht geändert werden, wodurch die Sicherheitsaktualisierungen einfacher und kostengünstiger zu implementieren sind. Aus diesem Grund sind passive IDS der bevorzugte Ansatz bei der Betrachtung von Systemen und Einrichtungen, welche bereits errichtet sind oder Endgeräte „ohne IDS“ verwenden.

Bild 2 veranschaulicht zwei passive Beobachtungspunkte im lokalen und im entfernten (remote) Netzwerk, dargestellt als zwei blaue Punkte.

Rein passive IDS haben eine eingeschränkte Fähigkeit zum Erkennen von Eindringungen, da sie möglicherweise nicht „gewahr sind“, was normaler Datenverkehr in typischen Operationen von Energiesystemen ist. Zusätzlich zu diesen passiven IDS können jedoch NSM-Datenobjekte sowohl in Systemen implementiert werden, welche die Anwendung und Kommunikationsstapel aufnehmen, als auch in Intermediate Systems (IS) (siehe die vielen roten Punkte in Bild 2). Diese NSM-Datenobjekte würden zusätzliche Informationen bereitstellen, um zu bestimmen, ob ein Angriff bevorsteht, welche Art von Angriff stattfindet und die Zeit des kritischen Ereignisses.

Die NSM-Datenobjekte in einem vorhandenen System würden einfach verfügbare Informationen einbeziehen, welche unter Verwendung des bestehenden Protokolls als zusätzliche Daten gesendet werden könnten. Häufig sind diese Daten verfügbar, werden jedoch entweder ignoriert oder in einem lokalen Protokoll als „Fehler“ gespeichert. Der Schlüssel ist die Identifizierung der wichtigen, aber verfügbaren Daten und deren Bereitstellung an ein IDS oder ein Sicherheitssystem.

5.6.3 IDS: Architektur einer aktiven Sicherheitsüberwachung mit NSM-Datenobjekten

Aktive Sicherheitsüberwachung umfasst die Auslegung der Netzwerke und der Endsysteme mit einer Sicherheitsüberwachung als Teil der Entwurfskriterien. Statt sich darauf zu verlassen, welche Fehlerprüfung in

vorhandenen Systemen verfügbar ist, schließen diese Systeme in ihrer Auslegung die Fähigkeit zum Identifizieren und Bereitstellen von zusätzlichen Sicherheitsinformationen an einen „Sicherheitsmanager“ ein, einschließlich Informationen zu ungewöhnlichen Ereignissen, nicht autorisierten Nachrichten, Daten mit möglichem Bezug zu DoS-Angriffen, usw.

In dieser Architektur einer aktiven Sicherheitsüberwachung würde jede Schicht im Protokollstapel auf mögliche Angriffe auf die Sicherheit überwachen, und viele Anwendungen würden Schlüsseldaten zu Fehlern und Ausfällen liefern.

Ein Sicherheitsprovider würde die NSM-Datenobjekte verwalten, wobei möglicherweise zweckmäßige Schwellenwerte, Grenzwerte und andere Parameter eingestellt würden, um eine Feinabstimmung des Antwortverhaltens zu erreichen, die besser zur Betriebsumgebung jedes Energienetzes passt. Bei Erkennen einer Funktionsabweichung würden diese NSM-Daten zur weiteren Analyse an den Sicherheitsmanager gesendet.

Diese Architektur ist vergleichbar mit der SNMP-Architektur. Dies bedeutet jedoch nicht, dass das SNMP-Format notwendigerweise für die Übermittlung von NSM-Daten verwendet wird: die NSM-Datenobjekte würden unter Verwendung des Protokolls implementiert, welches für andere Typen der Kommunikation verwendet wird.

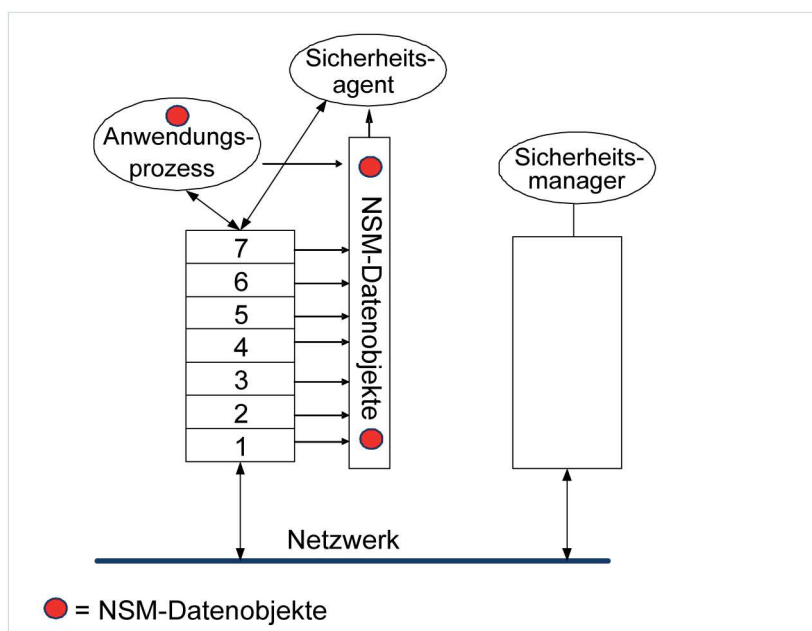


Bild 3 – Architektur einer aktiven Sicherheitsüberwachung mit NSM-Datenobjekten

5.7 Ende-zu-Ende Sicherheit

5.7.1 Konzepte der Ende-zu-Ende-Sicherheit

Ende-zu-Ende-Sicherheit umfasst nicht nur vorsätzliche Angriffe sondern auch versehentliche Handlungen.

Diese Aussage ist wesentlich für das Verständnis des Anwendungsbereichs der vorliegenden Norm. Obwohl einige Definitionen von „Sicherheit“ lediglich den Schutz von Systemen gegen vorsätzliche Angriffe durch Terroristen oder Cyberhacker einschließen, wird häufig größerer Schaden durch Unachtsamkeit, Geräteausfall oder Naturkatastrophen verursacht als durch diese vorsätzlichen Angriffe. Deshalb deckt „Sicherheit“ in der vorliegenden Norm alle Gefährdungen ab, einschließlich vorsätzlicher Angriffe, versehentlicher Fehler, Geräteausfall, Softwareproblemen und Naturkatastrophen. Für die Sicherheit und Zuverlässigkeit der Betriebsabläufe von Energiesystemen spielt es keine Rolle, ob ein Problem durch einen vorsätzlichen Angriff oder durch einen versehentlichen Fehler verursacht wurde.

Außerdem können viele der gleichen Maßnahmen, welche gegen vorsätzliche Angriffe angewendet werden könnten, gegen versehentliche Fehler angewendet werden. Folglich ist es nützlich und kostengünstig beide Typen von Sicherheitsbedrohungen mit den gleichen Typen von Sicherheitsmaßnahmen anzugehen.

Ende-zu-Ende-Sicherheit bringt einen viel größeren Anwendungsbereich mit sich, als die Authentifizierung von Nutzern und die Sicherstellung des Protokolls. Ende-zu-Ende-Sicherheit umfasst Sicherheitsstrategien, Zugriffskontrollmechanismen, Schlüsselmanagement, Auditprotokolle und andere kritische Aspekte des Schutzes von Infrastruktur. Sie umfasst auch die Sicherung der Informationsinfrastruktur selbst.

Wie in IEC/TS 62351-1 behandelt, umfassen Sicherheitsbedrohungsagenten:

- a) Versehentlich: Bedrohungsagenten, welche versehentliche „Angriffe“ auf das System verursachen:
 - unachtsame Nutzer;
 - Angestellte, welche Sicherheitsmaßnahmen umgehen;
 - Ausfälle von Sicherheitssystemen;
 - Ausfall von Einrichtungen;
 - Naturkatastrophen.
- b) Vorsätzlich: Bedrohungsagenten, welche vorsätzlich Angriffe unternehmen:
 - verärgerte Angestellte;
 - Industriespionageagenten;
 - Vandalen;
 - Cyberhacker;
 - Viren und Würmer;
 - Diebe;
 - Terroristen.

Der wesentliche Punkt ist, dass die Gesamtsicherheit von Betriebsabläufen von Energiesystemen nicht nur durch vorsätzliche Terrorakte bedroht wird, sondern durch viele andere, manchmal vorsätzliche, manchmal versehentliche Bedrohungen, welche letztendlich verheerendere Folgen haben können als direkte Spionage.

Wie in IEC/TS 62351-1 angemerkt, bietet die Sicherung von Protokollen unter Verwendung von IEC 62351 Authentifizierung und (für einige Protokolle) Verschlüsselung über die Kommunikationsverbindung, wobei 3 der 4 Sicherheitsanforderungen abgedeckt werden: Integrität, Vertraulichkeit und Unleugbarkeit. Diese sehr wichtigen Sicherheitsmaßnahmen lassen jedoch kritische Lücken:

- Erstens, decken sie nur die Protokolle über die Kommunikationsverbindung ab, und befassen sich nicht mit den Endnutzern und Endgeräten. Getarnte Nutzer, Geräteausfälle oder nicht erkannte Eindringungen kann die Betriebsabläufe sogar dann stören, wenn die Datenaustausche ordnungsgemäß fortgeführt werden.
- Zweitens, befassen sie sich nicht mit Dienstverweigerung. Dienstverweigerung kann viele Formen annehmen, von verlangsamten Datenaustauschen, Geräteausfällen, Fehler in Kommunikationspfaden, unregelmäßige oder verminderte Verfügbarkeit bis Störung und Diebstahl.

Obwohl das Hauptziel von Sicherheitsmaßnahmen möglicherweise die Verhinderung von Angriffen auf die Sicherheit ist, können Sicherheitsmaßnahmen nicht ausschließlich vorbeugend sein. Wenn nur eine Verhinderung angestrebt würde, hätten Angreifer, wenn (und es gibt immer ein wenn) es ihnen gelingt in eine Peripherie einzudringen, die vollständige Freiheit jegliche Beschädigungen zu verursachen die sie beabsichtigen. Folglich sollte „Verhinderung“ von Angriffen sowohl als Abhalten als auch Aufhalten von Angriffen verstanden werden. Zusätzlich muss ein Sicherheitsschutz für Gegenangriffe, welche nicht abgehalten wurden, bereitgestellt werden.

5.7.2 Rolle von Netzwerk- und Systemmanagement (NSM) in Ende-zu-Ende-Sicherheit

Ende-zu-Ende-Sicherheit umfasst mehr als die Verschlüsselung und Authentifizierung, welche die primären Sicherheitsmethoden sind. Wie in IEC/TS 62351-1 behandelt und in Bild 5 dargestellt, muss die gesamte

Informationsinfrastruktur sicher und zuverlässig gestaltet werden, um Sicherheit und Zuverlässigkeit von Betriebsabläufen von Energiesystemen bereitzustellen. Bild 5 stellt das Management sowohl der Infrastruktur des Energiesystems als auch der Informationsinfrastruktur dar.

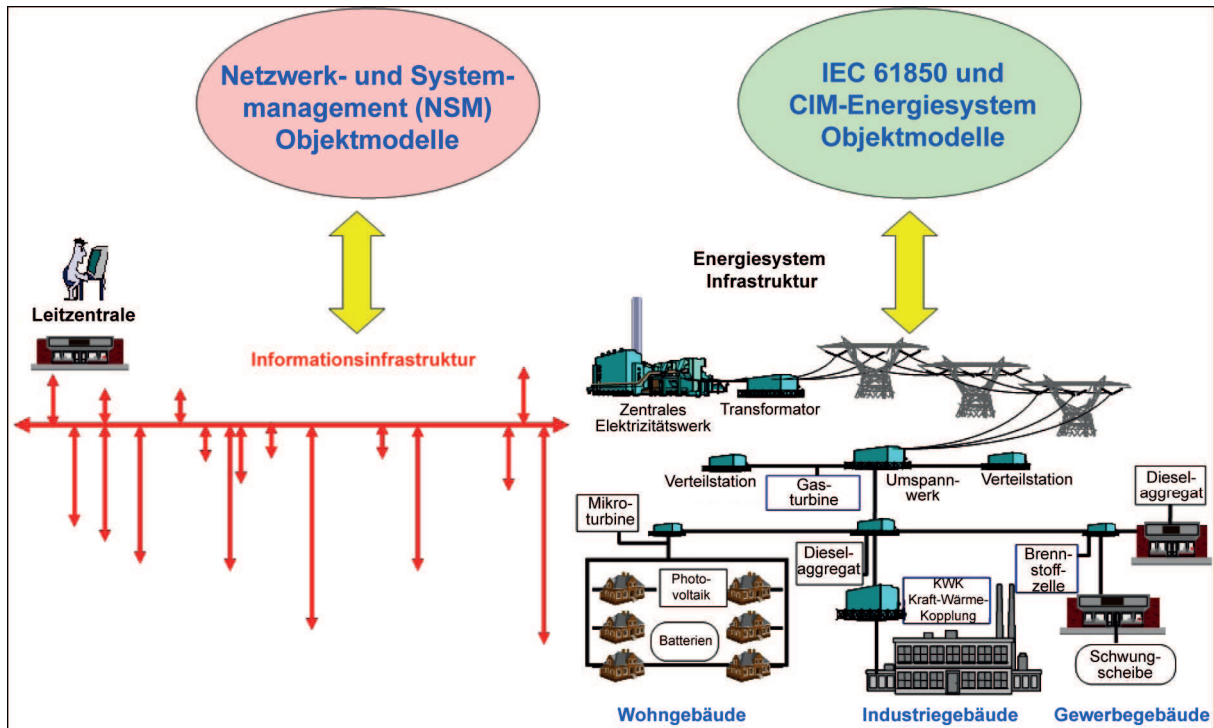


Bild 4 – Vergleich von NSM-Datenobjekten mit Objekten nach IEC 61850

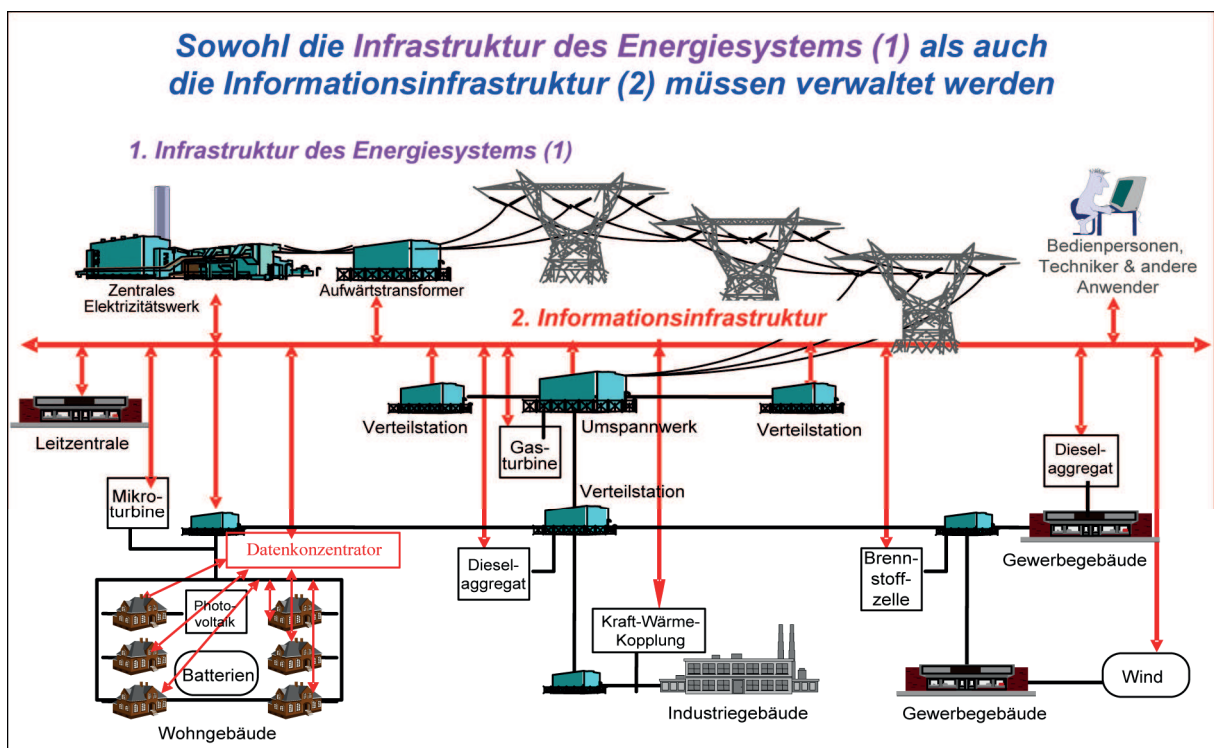


Bild 5 – Management beider Infrastrukturen von Systemen der Energietechnik

Nicht alle dieser Sicherheits- und Zuverlässigkeitsanforderungen können durch Netzwerk- und Systemmanagement (NSM) erfüllt werden, aber viele von ihnen können verbessert werden. Insbesondere die folgenden Funktionen können durch NSM bereitgestellt werden:

- Überwachung des Status von Softwareanwendungen, Hardwareeinrichtungen und Kommunikation. Diese Statusüberwachung kann Meldungen in Bezug auf Änderungen bereitstellen, wie z. B. Geräteausfall, nicht bestimmungsgemäße Konfigurationsänderungen, „Abstürze“ oder Ausfälle von Software, vorübergehende Kommunikationsstörungen und dauerhafte Kommunikationsausfälle.
- Überwachung des Betriebsverhaltens von Systemen und Kommunikation. Diese Überwachung des Betriebsverhaltens kann Zustände des Datenverkehrs, Änderungen des Leistungsvermögens von Softwareanwendungen, Änderungen des Datendurchsatzes, Leistungsergebnisse aufgrund von Konfigurationsänderungen, usw. aufzeichnen.
- Erkennen von Eindringungen. Zusätzlich zu offensichtlichen Eindringungen muss diese Erkennung empfindlich in Bezug auf „normale“ Bedingungen sein, um zu versuchen, geringfügige Änderungen der Zustände zu erkennen, welche auf eine Eindringung hinweisen könnten.
- Konfigurationsmanagement. Die Konfiguration von Kommunikationsnetzen und Einrichtungen kann entweder durch Herstellen automatischer Änderungen auf der Grundlage von Ereignissen (z. B. Wechsel zum Backup-Kanal bei Ausfall des Primärkanals) oder durch manuelle Änderung der Konfiguration, wie z. B. ein Geräteteil außer Betrieb nehmen und durch ein anders ersetzen) gesteuert werden.

5.8 NSM-Anforderungen: Erkennungsfunktionen

5.8.1 Erkennen unbefugten Zugriffs

Die grundlegendste Anforderung an Eindringungserkennung ist das Ermitteln, ob eine unbefugte Person versucht auf das System zuzugreifen. Diese Anforderung basiert folglich auf der Festlegung, welche Personen befugt sind, wodurch angegeben wird, welche Personen unbefugt sind.

Die NSM-Datenobjekte, welche zum Erkennen von unbefugtem Zugriff erforderlich sind, umfassen:

- Ermitteln, dass ein unbefugter Nutzer versucht eine Verbindung aufzubauen oder eine Nachricht zu übermitteln, auf der Grundlage einer Liste von befugten Nutzern der Verbindungen.

5.8.2 Erkennen einer Ressourcenüberlastung als einen Dienstverweigerungsangriff (DoS)

Üblicherweise kann das passive IDS eine Ressourcenüberflutung auf der Grundlage von Zeit und/oder Bandbreitebelastung (z. B. vergleichbar mit einem SYN-Flutungsangriff) erkennen. Dies funktioniert gut bei in Bezug auf Ressourcen „unbeschränkten“ Geräten, aber nicht so gut innerhalb der TC57-Domäne, wo Kommunikationsressourcen eingeschränkt sind. Die Gründe sind die Folgenden:

- In typischen Netzwerken kann ein IDS in der Lage sein einen SYN-Flutungsangriff zu erkennen, bei welchem Hunderte oder Tausende von schnellen SYN verwendet werden (z. B. ein Angriff, der so geplant ist, dass verfügbare TCP-Verbindungen belastet werden). In Netzwerken der TC57-Domäne unterstützen jedoch Geräte nach IEC 60870-5-104, IEC 60870-6 und IEC 61850 nicht Hunderte oder Tausende von Verbindungen.
- Aufgrund der geringeren Anzahl verfügbarer Verbindungen muss der Zeitrahmen, der zur Entsprechung eines SYN-Flutungsangriffs erforderlich ist, kürzer sein, und möglicherweise würden alle passiven IDS nicht in der Lage sein, den Angriff zu erkennen. Eine mögliche Lösung könnte es sein, diese passiven IDS auf der Grundlage der erwarteten Ressourcenkapazität zu konfigurieren, wobei dies jedoch die Konfiguration und die Instandhaltung des Kommunikationsnetzes erschwert, da die IDS jedes Mal bei ihrer Neukonfiguration ebenfalls aktualisiert werden müssten.
- Eine alternative Lösung ist es, dem Netzwerk die dynamische Neukonfiguration in Bezug darauf, was einen SYN-Flutungsangriff darstellen könnte, selbst zu überlassen. Der COMM-Stapel und Anwendungen haben explizite Kenntnisse bezüglich der Ressourcen und diese expliziten Kenntnisse bezüglich der Ressourcen können durch genormte NSM-Datenobjekte abgerufen werden.

Die NSM-Datenobjekte, die zum Erkennen von Angriffen mit Ressourcenüberflutung erforderlich sind, umfassen:

- Überschreiten der maximalen Anzahl von über das Netzwerk zulässigen Verbindungen;
- Zählung der Anzahl von tatsächlich über das Netzwerk eingerichteten Verbindungen;
- Überschreiten der maximalen Anzahl von Verbindungen, welche gleichzeitig verwendet werden können;
- Zählung der Anzahl von tatsächlich gleichzeitig verwendeten Verbindungen;
- Überschreiten von CPU-Belastungsgrenzwerten;
- Überschreiten von Grenzwerten der Speichernutzung.

Diese Informationen müssen von jedem „Knoten“ entlang des gesamten Kommunikationspfades zwischen Anwendungen gesammelt werden, da unterschiedliche Kommunikationsabschnitte zwischen Knoten betroffen sein und einen Engpass verursachen könnten.

5.8.3 Erkennen von DoS-Angriffen mit ungültigem Pufferzugriff

Passive IDS sind nicht intrinsisch dazu in der Lage, zu bestimmen, ob ein Angriff mit Pufferüberlauf bevorsteht. Dies gilt insbesondere für TASE.2 nach IEC 61850 und IEC 60870-6, wo die Größe des Anwendungspuffers in Bezug auf die Laufzeit verhandelt wird. Der Anwendungs-/Kommunikationsstapel könnte jedoch solcher Überläufe gewahr sein. Dies gilt sogar für Ethernet-Puffer-Fragen innerhalb des Kommunikationsstapels.

Die NSM-Datenobjekte, welche zum Erkennen von Angriffen mit Puffer-Überlauf/Unterlauf erforderlich sind, umfassen:

- Anzahl von Überläufen;
- Anzahl von Unterläufen;
- Auditfähigkeit zum Erkennen, welche Quelle den Puffer-Überlauf/Unterlauf verursacht hat.

5.8.4 Erkennen von verfälschten/fehlerhaften PDU

Passive IDS können die Fähigkeit besitzen, einige fehlerhafte Pakete zu erkennen. Es ist jedoch nahezu unmöglich für IDS ein Paket zu erkennen, welches verfälscht wurde (z. B. man-in-the-middle (de: Mittelsmann)). Zusätzlich dürfen passive IDS bei komplexeren Protokollen der Anwendungsebene (z. B. TASE.2 nach IEC 60870-5, IEC 61850 und IEC 60870-6) nicht die Fähigkeit zum Erkennen aller möglichen fehlerhaften Pakete besitzen, welche Verarbeitungsprobleme verursachen könnten. Der Kommunikationsstapel, Anwendung, und/oder IS haben jedoch diese Kenntnisse, da sie jedes Paket interpretieren müssen.

Die NSM-Datenobjekte in dieser Kategorie umfassen:

- Anzahl von erkannten fehlerhaften PDU;
- Anzahl von PDU, welche verfälscht wurden;
- Auditfähigkeit zum Erkennen, welche Quelle die verfälschten/fehlerhaften PDU verursacht hat.

5.8.5 Erkennen der Störung des physikalischen Zugriffs

Wenn eine Ressource ausgeschaltet oder vom Kommunikationsnetz getrennt wurde, stellt dies einen ultimativen DoS-Angriff dar, da eine physikalische Wiederherstellung erforderlich sein könnte. Insbesondere dann, wenn das Gerät nicht per Fernwirkung wieder eingeschaltet werden kann, ist es entscheidend, in der Lage zu sein, die Zeit des Ausschaltungs-/Abtrennungs-Ereignisses genau zu protokollieren und dieses zu anderen Ereignissen in Beziehung zu setzen.

Die NSM-Datenobjekte, welche zum Erkennen von Störungen des physikalischen Zugriffs erforderlich sind, umfassen:

- Ausfall der Stromversorgung für Geräte und Zeit des Ausfalls;
- abgetrennte Medien und Zeit der Abtrennung;
- wiederhergestellte Stromversorgung für Geräte und Zeit der Wiederherstellung;
- wieder verbundene Medien und Zeit der Wiederverbindung;

5.8.6 Erkennen eines ungültigen Netzwerkzugriffs

Firewalls sind so ausgelegt, dass ein ungültiger Zugriff auf Netzwerke verhindert wird, insbesondere durch Verwendung von Zugriffskontrolllisten, welche nur befugten IP-Adressen den Durchlass durch die Firewall gewähren. Andere Firewall-Fähigkeiten umfassen Port-Einschränkungen, zustandsabhängige Filterung und Session-Management.

Interne Ressourcen (z. B. hinter der Firewall) können jedoch (versehentlich oder vorsätzlich) in Angreifer umgewandelt werden. In vielen Situationen kann diese Art der „Umwandlung“ durch passive IDS erkannt werden. IDS innerhalb des Netzwerks sind jedoch möglicherweise nicht in der Lage, stattfindende ungültige Datenaustausche zu erkennen. Zum Beispiel, könnten jegliche Protokolle, welche sowohl intern als auch extern verwendet werden, wie z. B. IEC 60870-6 (TASE.2) und jetzt IEC 61850 zwischen Stationen und Leitzentralen, böswillige Daten von einer externen Quelle (welche nur für bestimmte Datentypen vertrauenswürdig ist) an eine interne Ressource übermitteln, von wo sie möglicherweise als vollständig vertrauenswürdige Daten an andere interne Ressourcen gesendet werden.

Ein großer Teil des Schutzes gegen diesen Typ von Angriffen müsste innerhalb der tatsächlichen Anwendungen erfolgen, welche den Datenaustausch zwischen externen und internen Ressourcen abwickeln. Diese Anwendungen sollten Kenntnisse darüber haben, welche Daten gültig und/oder ungültig sind. Einige NSM-Datenobjekte, welche den Datenverkehr zwischen Anwendungen/Systemen überwachen, könnten dieses Bestreben jedoch unterstützen.

Die NSM-Datenobjekte, welche zur Unterstützung des Erkennens eines ungültigen Netzwerkzugriffs erforderlich sind, umfassen:

- unerwartete Dichte von Datenverkehr zwischen spezifischen Anwendungen/Systemen im Netzwerk;
- unerwarteter Umfang von Datenverkehr zwischen spezifischen Anwendungen/Systemen im Netzwerk;
- Erkennen verdächtiger Daten (Virus, Wurm oder fehlerhafte Daten).

5.8.7 Erkennen koordinierter Angriffe

Koordinierte Angriffe über mehrere Stationen, Leitzentralen und Versorgungsunternehmen könnten mehr Schaden zufügen, als diese gleichen Angriffe verursachen würden, wenn sie zu/an unterschiedlichen Zeiten oder Standorten ausgeführt würden. Wenn aufeinanderfolgende Angriffe im Gange sind, könnte es entscheidend sein, in geeigneter Weise und zeitnah auf den ersten Angriff zu reagieren, um die Auswirkungen der restlichen Angriffe abzuschwächen.

Ungeachtet dessen, ob spezifische Angriffe erfolgreich waren oder nicht, kann die Kenntnis, dass sie koordiniert waren, wichtige Anhaltspunkte dafür liefern, wer sie veranlasst hat, wie sie ausgeführt wurden und warum sie stattgefunden haben.

Deshalb muss ein Mechanismus zum Schaffen eines Zusammenhangs zwischen Informationen normiert werden. Konzeptionell ist ein solcher Mechanismus einfach: ein vollständiges Protokoll aller maßgeblichen Alarme und Ereignisse (einschließlich Ereignisse, welche stattfinden sollten, jedoch nicht auftraten oder fehlgeschlagen sind), mit synchronisierten und genauen Zeitstempeln.

In der Praxis wiesen die Präzision, Zeitzone, und Genauigkeit von Zeitstempeln erhebliche Abweichungen auf. Folglich sollten Normen zu Zeitstempeln ein Zeitformat nach ISO 8601 verwenden, mit der Fähigkeit zum Aufzeichnen mit einer Präzision im Millisekundenbereich, und mit einer angemessen genauen Zeitsynchronisierung über Systeme hinweg. Diese Zeitsynchronisierung könnte für einige Funktionen im Bereich von 1 ms liegen, sollte jedoch für die meisten anderen Funktionen mindestens im Bereich von ein paar Sekunden liegen.

Die NSM-Datenobjekte, welche zur Unterstützung des Erkennens koordinierter Angriffe erforderlich sind, umfassen:

- Identifizierung aller Kommunikationsausfälle;
- Identifizierung aller Ausfälle von Endsystemen;
- Identifizierung aller Dos-Angriffe;
- Zeitstempel mit einer Präzision im Millisekundenbereich an allen Datenobjekten;
- Zeitsynchronisierung über alle Kommunikations- und Endsysteme.

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 present Part 7 of IEC 62351 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:

FDIS	RVD

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

- 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.

Document history

Any person intervening in the present document is invited to complete the table below before sending the document elsewhere. The purpose is to allow all actors to see all changes introduced and the intervening persons.

Any important message to IEC editors should also be included in the table below.

Name of intervening person	Document received		Brief description of the changes introduced	Document sent	
	From	Date		To	Date
G.L.Pugni		19/11/2013	Added 5.6		
F. Alvarez		19/11/2013	Modified chapter 5		
S.Fries		19/11/2013	Comments on chapter 6		
S.Fries		13/12/2013	Modified chapter 6		
G.L.Pugni/F.Bellio		13/12/2013	Modified chapter 7 and chapter 8 according to EPRI document		
G.L.Pugni/F.Bellio		10/01/2014	Modified chapter 8 according EPRI document structure		
F.Alvarez		01/03/2014	Rewritten chapter 5 (including also former chapter 6)		
G.L.Pugni/F.Bellio/F.Alvarez		14/04/2014	Rewritten chapter 6 and 7 with Abstract Object UML notation generated.		
G.L.Pugni/F.Bellio/F.Alvarez		04/05/2014	UML Model updated,		
H.Falk		04/07/2014	UML Model updated with clock section		
G.L.Pugni, F.Bellio, H.Falk		30/07/2014	Chapter 5 updated, introduced sections 5.10, 5.11, 5.12		
G.L.Pugni, F.Bellio		16/09/2014	UML Model updated		
G.L.Pugni, F.Bellio, F.Alvarez		06/09/2014	UML Model updated: Common Attributes summarized, introduced Interfaces Agent.		
F. Alvarez, Fernando Alvarez, Giovanna Dondossola		20/10/2014	UML Model review, Informative section review.		
Giovanna Dondossola, G.L.Pugni		01/12/2014	Sections 5.1-5.7 (now 5.1 – 5.5) review. Partial 5.8 - 5.9 review from Fernando. Sections 5.10-5.12 (now 5.8 – 5.10) review. UML model updated and extended including event notification.		
G.L.Pugni		17/12/2014	Cleanup and consolidation before CD		
Frances Cleveland		20/12/2014	Editorial updates		
Margareta Nöth	G.L. Pugni	2015-01-12	CD document	CO	2015-01-13

CONTENTS

Document history	iii
Table of Figures	5
Table of Tables.....	6
1 Scope.....	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviation and Acronyms	2
5 Introduction to Network and System Management (NSM) (informative).....	3
5.1 Objectives	3
5.2 NSM Concepts	4
5.2.1 Simple Network Management Protocol (SNMP)	4
5.2.2 ISO NSM categories	5
5.2.3 NSM “data objects” for power system operations	5
5.3 Communication network management	5
5.3.1 Network configuration	5
5.3.2 Network backup	6
5.3.3 Communications failures and degradation	6
5.4 Communication protocols.....	7
5.5 End systems management.....	7
5.6 Intrusion detection systems (IDS).....	8
5.6.1 IDS guidelines	8
5.6.2 IDS: Passive observation techniques	9
5.6.3 IDS: Active security monitoring architecture with NSM data objects	9
5.7 End-to-end security	10
5.7.1 End-to-end security concepts	10
5.7.2 Role of network and system management (NSM) in end-to-end security	11
5.8 NSM requirements : detection functions	13
5.8.1 Detecting unauthorized access	13
5.8.2 Detecting resource exhaustion as a denial of service (DoS) attack	13
5.8.3 Detecting invalid buffer access DoS attacks	14
5.8.4 Detecting tampered/Malformed PDUs	14
5.8.5 Detecting physical access disruption	14
5.8.6 Detecting invalid network access	14
5.8.7 Detecting coordinated attacks.....	15
5.9 Abstract Object and Agent UML description	15
5.9.1 Purpose of UML.....	15
5.9.2 Abstract Types and Base Types	16
5.9.3 Enumerated Types	17
5.9.4 Abstract Agents	17
5.9.5 Unsolicited Event Notification	20
5.10 Abstract Object UML translation towards SNMP	21
5.10.1 Simple Network Management Protocol (SNMP)	21
5.10.2 Management information bases (MIBs).....	21
5.11 SNMP mapping of UML model Objects	22
5.12 SNMP transport and Security	24
6 Abstract objects (normative).....	27
6.1 Package Abstract Types	27

6.1.1	General	27
6.1.2	BooleanValue	27
6.1.3	BooleanValueTs	27
6.1.4	CounterTs	28
6.1.5	CntRs root class	28
6.1.6	Floating	28
6.1.7	FloatingTs	28
6.1.8	EntityIndex root class	29
6.1.9	Integer	29
6.1.10	UnsignedInt root class	29
6.1.11	IntegerTs	29
6.1.12	InetAddress root class	30
6.1.13	InetAddressType root class	30
6.1.14	MacAddress root class	30
6.1.15	Selector root class	30
6.1.16	Timestamp root class	31
6.1.17	CharString	31
6.1.18	CharStringTs root class	31
6.2	Package EnumeratedTypes	31
6.2.1	General	31
6.2.2	AppDatStKind enumeration	31
6.2.3	ExtKind enumeration	32
6.2.4	IntKind enumeration	32
6.2.5	LnkKind enumeration	32
6.2.6	PSPAccKind enumeration	33
6.2.7	ProtIdKind enumeration	33
6.2.8	EventKind enumeration	33
6.2.9	TimSyncIssueKind enumeration	34
6.2.10	TimSyncSrcKind enumeration	34
6.2.11	AppDatStType root class	34
6.2.12	ExtType root class	35
6.2.13	IntType root class	35
6.2.14	EventType root class	35
6.2.15	PSPAccType root class	35
6.2.16	ProtIdType root class	35
6.2.17	TimSyncIssueType root class	36
6.2.18	TimSyncSrcType root class	36
6.2.19	LnkType root class	36
6.3	Package Common Objects	37
6.3.1	General	37
6.3.2	ProtocolAndSecurityInfo	37
6.3.3	SecurityInfo root class	38
7	Agents	38
7.1	Package Overview	38
7.2	Package Environmental Agent	40
7.2.1	General	40
7.2.2	Environmental root class	40
7.2.3	PSUPEntry root class	41
7.2.4	Notification root class	41
7.2.5	SecurityNotification root class	42

7.3	Package Device Agent	43
7.3.1	General	43
7.3.2	Device	44
7.3.3	CPUEntry root class	45
7.3.4	EXTEntry root class	45
7.3.5	STOREEntry root class	46
7.3.6	Notification root class	46
7.3.7	SecurityNotification root class	47
7.4	Package Application Protocols Agents	47
7.4.1	General	47
7.4.2	Package IEEE1815 and IEC870-5 Agent	49
7.4.2.1	General	49
7.4.2.2	60870andDNPProtocolInfo	50
7.4.2.3	Summary	51
7.4.2.4	Association	52
7.4.2.5	MasterAssociation	53
7.4.2.6	OutstationAssociation	54
7.4.2.7	60870andDNPSecurityNotification root class	56
7.4.2.8	60870andDNPNotification root class	56
7.4.3	Package IEC61850 Agent	56
7.4.3.1	General	56
7.4.3.2	61850SecurityInfo	57
7.4.3.3	GSEandSVProvider	57
7.4.3.4	GSEandSVProtocolAssociation	58
7.4.3.5	GSEandSVSecurityNotification root class	59
7.4.3.6	GSEandSVNotification root class	59
7.4.3.7	Package AC SI	60
7.4.3.7.1	General	60
7.4.3.7.2	ACSISummary	61
7.4.3.7.3	ACSISecurityNotification root class	62
7.4.3.7.4	ACSINotification root class	62
7.4.3.8	Package MMS	63
7.4.3.8.1	General	63
7.4.3.8.2	MMSPProvider	64
7.4.3.8.3	MMSAssociation	65
7.4.3.8.4	MMSProtocolInfo	65
7.4.3.8.5	MMSSecurityNotification root class	66
7.4.3.8.6	MMSNotification root class	67
7.4.3.9	Package SV	68
7.4.3.9.1	General	68
7.4.3.9.2	SVProvider	68
7.4.3.9.3	SVAssociation	69
7.4.3.9.4	SVSecurityNotification	70
7.4.3.9.5	SVNotification	70
7.4.3.10	Package GSE	71
7.4.3.10.1	General	71
7.4.3.10.2	GSEProvider	71
7.4.3.10.3	GSEAssociation	72
7.4.3.10.4	GSESecurityNotification	72
7.4.3.10.5	GSENotification	73

7.5	Package Interfaces Agent.....	74
7.5.1	General	74
7.5.2	Interfaces root class	75
7.5.3	ETHEntry.....	76
7.5.4	KEYEntry.....	76
7.5.5	SEREntry	76
7.5.6	ALGEntry.....	77
7.5.7	USBEntry	77
7.5.8	Interface root class	77
7.5.9	Notification root class	78
7.6	Package Clocks Agent	79
7.6.1	General	79
7.6.2	Clock root class	79
7.6.3	ClocksEntry root class	80
7.6.4	Notification root class	80
7.6.5	SecurityNotification root class.....	80
7.7	Network and Transport Agents.....	81
7.7.1	TCP.....	81
7.7.2	UDP	81
7.7.3	IP	81
8	SNMP Security	82
9	References and bibliography.....	83
Annex A	: SNMP MIB Mapping	85

Table of Figures

Figure 1 - Example of a power system SCADA architecture extended with NSM Data Objects	4
Figure 2 - IDS Information exchange between applications: generic communication topology8	8
Figure 3 - Active security monitoring architecture with NSM data objects	10
Figure 4 - Comparison of NSM data objects with IEC 61850 objects	12
Figure 5 - Management of both the power system infrastructure	12
Figure 6 - Abstract Types	16
Figure 7 - Enumerated Types	17
Figure 8 - Subagents	18
Figure 9 - Agent	19
Figure 10 - Model Stereotypes	20
Figure 11 - MIB hierarchy	22
Figure 12 - SNMP Table	23
Figure 13 - SNMP RFCs map and security	25
Figure 14 - SNMP Entity	26
Figure 15 – Class diagram Common Objects::Common Objects	37
Figure 16 – Class diagram Overview::Part7 Classes Overview	39
Figure 17 – Class diagram Environmental Agent::Environmental	40
Figure 18 – Class diagram Device Agent::Device	43
Figure 19 – Class diagram IEEE1815 and IEC870-5 Agent::DNP and 60870 Agent Relationships	49
Figure 20 – Class diagram ACSI::ACSI	60
Figure 21 – Class diagram MMS::MMS	63
Figure 22 – Class diagram SV::SV	68
Figure 23 – Class diagram GSE::GSE	71
Figure 24 – Class diagram Interfaces Agent::Interfaces	74
Figure 25 – Class diagram Clocks Agent::Clocks Agent	79

Table of Tables

Table 1 – Attributes of Abstract Types::BooleanValue	27
Table 2 – Attributes of Abstract Types::BooleanValueTs	27
Table 3 – Attributes of Abstract Types::CounterTs	28
Table 4 – Attributes of Abstract Types::CntRs	28
Table 5 – Attributes of Abstract Types::Floating	28
Table 6 – Attributes of Abstract Types::FloatingTs	28
Table 7 – Attributes of Abstract Types::EntityIndex	29
Table 8 – Attributes of Abstract Types::Integer	29
Table 9 – Attributes of Abstract Types::UnsignedInt	29
Table 10 – Attributes of Abstract Types::IntegerTs	29
Table 11 – Attributes of Abstract Types::InetAddress	30
Table 12 – Attributes of Abstract Types::InetAddressType	30
Table 13 – Attributes of Abstract Types::MacAddress	30
Table 14 – Attributes of Abstract Types::Selector	30
Table 15 – Attributes of Abstract Types::Timestamp	31
Table 16 – Attributes of Abstract Types::CharString	31
Table 17 – Attributes of Abstract Types::CharStringTs	31
Table 18 – Literals of EnumeratedTypes::AppDatStKind	31
Table 19 – Literals of EnumeratedTypes::ExtKind	32
Table 20 – Literals of EnumeratedTypes::IntKind	32
Table 21 – Literals of EnumeratedTypes::LnkKind	32
Table 22 – Literals of EnumeratedTypes::PSPAccKind	33
Table 23 – Literals of EnumeratedTypes::ProtIdKind	33
Table 24 – Literals of EnumeratedTypes::EventKind	33
Table 25 – Literals of EnumeratedTypes::TimSyncIssueKind	34
Table 26 – Literals of EnumeratedTypes::TimSyncSrcKind	34
Table 27 – Attributes of EnumeratedTypes::AppDatStType	34
Table 28 – Attributes of EnumeratedTypes::ExtType	35
Table 29 – Attributes of EnumeratedTypes::IntType	35
Table 30 – Attributes of EnumeratedTypes::EventType	35
Table 31 – Attributes of EnumeratedTypes::PSPAccType	35
Table 32 – Attributes of EnumeratedTypes::ProtIdType	35
Table 33 – Attributes of EnumeratedTypes::TimSyncIssueType	36
Table 34 – Attributes of EnumeratedTypes::TimSyncSrcType	36
Table 35 – Attributes of EnumeratedTypes::LnkType	36
Table 36 – Attributes of Common Objects::ProtocolAndSecurityInfo	37
Table 37 – Attributes of Common Objects::SecurityInfo	38
Table 38 – Attributes of Environmental Agent::Environmental	40
Table 39 – Attributes of Environmental Agent::PSUPEntry	41
Table 40 – Attributes of Environmental Agent::Notification	41
Table 41 – Attributes of Environmental Agent::SecurityNotification	42
Table 42 – Attributes of Device Agent::Device	44
Table 43 – Attributes of Device Agent::CPUEntry	45
Table 44 – Attributes of Device Agent::EXTEntry	45
Table 45 – Attributes of Device Agent::STOREEntry	46
Table 46 – Attributes of Device Agent::Notification	46
Table 47 – Attributes of Device Agent::SecurityNotification	47
Table 48 – Attributes of IEEE1815 and IEC870-5 Agent::60870andDNPPProtocolInfo	50
Table 49 – Attributes of IEEE1815 and IEC870-5 Agent::Summary	51
Table 50 – Attributes of IEEE1815 and IEC870-5 Agent::Association	52
Table 51 – Attributes of IEEE1815 and IEC870-5 Agent::MasterAssociation	53

Table 52 – Attributes of IEEE1815 and IEC870-5 Agent::OutstationAssociation.....	54
Table 53 – Attributes of IEEE1815 and IEC870-5 Agent::60870andDNPSecurityNotification	56
Table 54 – Attributes of IEEE1815 and IEC870-5 Agent::60870andDNPNotification	56
Table 55 – Attributes of IEC61850 Agent::61850SecurityInfo	57
Table 56 – Attributes of IEC61850 Agent::GSEandSVProvider	57
Table 57 – Attributes of IEC61850 Agent::GSEandSVProtocolAssociation	58
Table 58 – Attributes of IEC61850 Agent::GSEandSVSecurityNotification	59
Table 59 – Attributes of IEC61850 Agent::GSEandSVNotification	59
Table 60 – Attributes of ACSI::ACSISummary	61
Table 61 – Attributes of ACSI::ACSISecurityNotification	62
Table 62 – Attributes of ACSI::ACSINotification.....	62
Table 63 – Attributes of MMS::MMSProvider.....	64
Table 64 – Attributes of MMS::MMSAssociation.....	65
Table 65 – Attributes of MMS::MMSProtocolInfo	66
Table 66 – Attributes of MMS::MMSSecurityNotification.....	66
Table 67 – Attributes of MMS::MMSNotification	67
Table 68 – Attributes of SV::SVProvider	68
Table 69 – Attributes of SV::SVAssociation	69
Table 70 – Attributes of SV::SVSecurityNotification	70
Table 71 – Attributes of SV::SVNotification.....	70
Table 72 – Attributes of GSE::GSEProvider	71
Table 73 – Attributes of GSE::GSEAssociation	72
Table 74 – Attributes of GSE::GSESecurityNotification	73
Table 75 – Attributes of GSE::GSENotification.....	73
Table 76 – Attributes of Interfaces Agent::Interfaces	75
Table 77 – Attributes of Interfaces Agent::ETHEntry	76
Table 78 – Attributes of Interfaces Agent::KEYEntry.....	76
Table 79 – Attributes of Interfaces Agent::SEREntry.....	76
Table 80 – Attributes of Interfaces Agent::ALGEntry.....	77
Table 81 – Attributes of Interfaces Agent::USBEntry	77
Table 82 – Attributes of Interfaces Agent::Interface.....	77
Table 83 – Attributes of Interfaces Agent::Notification	78
Table 84 – Attributes of Clocks Agent::Clock.....	79
Table 85 – Attributes of Clocks Agent::ClocksEntry	80
Table 86 – Attributes of Clocks Agent::SecurityNotification.....	81

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

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

1 Scope

This International Standard 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 goal is to define a set of Abstract Objects that will allow the remote monitoring of the health and condition of IEDs, RTUs, DER systems and other systems that are important to the power system operations.

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.

The telecommunication infrastructure that is in use for the transport of the telecontrol and automation protocols is already subject of health and condition monitoring control, using the concepts developed in the IETF Simple Network Management Protocol (SNMP) standards for network management; the power system specific devices (like teleprotection, telecontrol, substation automation, synchrophasors, inverters and protections) need instead a specific solution for their monitoring.

These objects will provide monitoring data on TC57 protocols running inside power systems (IEC 61850, IEC 60870-5-104) and device specific environmental and security status. Also IEEE 1815 DNP3 is included in the list of monitored protocols. The NSM data objects use the naming conventions developed for IEC 61850, expanded to address NSM issues. For sake of generality these data objects, and the data types of which they are comprised, are defined as abstract models of data objects.

In order to allow the integration of the monitoring of power system devices within the NSM environment in this standard a mapping of objects towards the SNMP protocol is provided.

The objects that are already covered by existing MIB will not be defined here but will be requested to be compliant to existing standards.

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*

IETF RFC 3416 SNMPv2

IETF RFC 5343 SNMPv3

IETF RFC 5591 TSM

IETF RFC 5592 SNMP over SSH

46 IETF RFC 5593 SNMP over DTLS or TLS

47 IETF RFC 6347 DTLS

48

49 3 Terms and definitions

50 Additional terms and definitions are in IEC 62351-2.

Term	Definition
Unified Modelling Language	Formal and comprehensive descriptive language with diagramming techniques used to represent software systems, from requirements analysis, through design and implementation, to documentation.
Structure of Management Information	An adapted subset of OSI's Abstract Syntax Notation One, ASN.1 used to write Management Information Base (MIB) modules (RFC 2578). The Structure of Management Information (SMIv2) defines fundamental data types, an object model, and the rules for writing and revising MIB modules (RFC 3410).
Transport Security Model	A Transport Security Model for the Simple Network Management Protocol for use with secure Transport Models in the Transport Subsystem (RFC 5590).
Datagram Transport Layer Security	A protocol that provides communications privacy for datagram protocols. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees (RFC 6347).

51

52 4 Abbreviation and Acronyms

53 Additional abbreviations and acronyms are in IEC 62351-2.

54

Term	Definition
NSM	Network and System Management
GIS	Geographical Information System
UML	Unified Modelling Language
ASN.1	Abstract Syntax Notation
SMI	Structure of Management Information
TSM	Transport Security Model
DTLS	Datagram Transport Layer Security

55

5 Introduction to Network and System Management (NSM) (informative)

5.1 Objectives

The information infrastructure in power operations consists not only of the communication networks, but also of the data that is exchanged between systems, stored in databases, and used by applications in power system operations. This information infrastructure is not typically treated as a coherent infrastructure, but is viewed as a disparate collection of communication channels, group of distinct network segments, separate devices, various databases, and different protocols. Often SCADA systems perform some communications monitoring, such as whether connections are available to their remote terminal units (RTUs), and they flag the event as connection lost when connections fail. However, real-time coherent, complete and homogeneous health status of the overall information infrastructure has been missing. Such real-time information infrastructure health status can support operators to detect and mitigate potential problems in the power system.

Traditionally, the information infrastructure supporting the power system has not been adequately monitored, and some corrective control actions are not possible. The analysis of past major blackouts showed that the primary reason behind the propagation of such blackouts after an initial equipment failure was the lack of critical information made available to the right user at the right time.

In the case of a communication network or system failure, possible cyber security attack, or other anomalous situation, maintenance personnel must be able to identify and diagnose the cause of the problems quickly: which equipment is affected, where the equipment is located, and what should be done to fix the problem. Power operators should be rapidly informed of such an anomalous occurrence in the information infrastructure.

Different organizations and utilities have different needs in what information is important for their information networks and which data should be available to their service and maintenance staff. For example, 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 configuration errors; application engineers must determine if applications have crashed, have not converged or are in an endless loop; cyber security personnel need to know where and which cyber-attack is affecting the network; and operators must filter out through large amounts of log data to determine if a possible “power system problem” is about to occur.

Network system management (NSM) data objects defined in this specification are specific and meaningful for the power industry and will provide end devices health information. These NSM data objects support communication network integrity, system, network and IED's health, Intrusion Detection Systems (IDS) and firewalls events, and other security/network management relevant information. An example high level architecture extending a typical

SCADA infrastructure of a power system with firewalls, intrusion detection systems and security monitoring objects is shown in Figure 1.

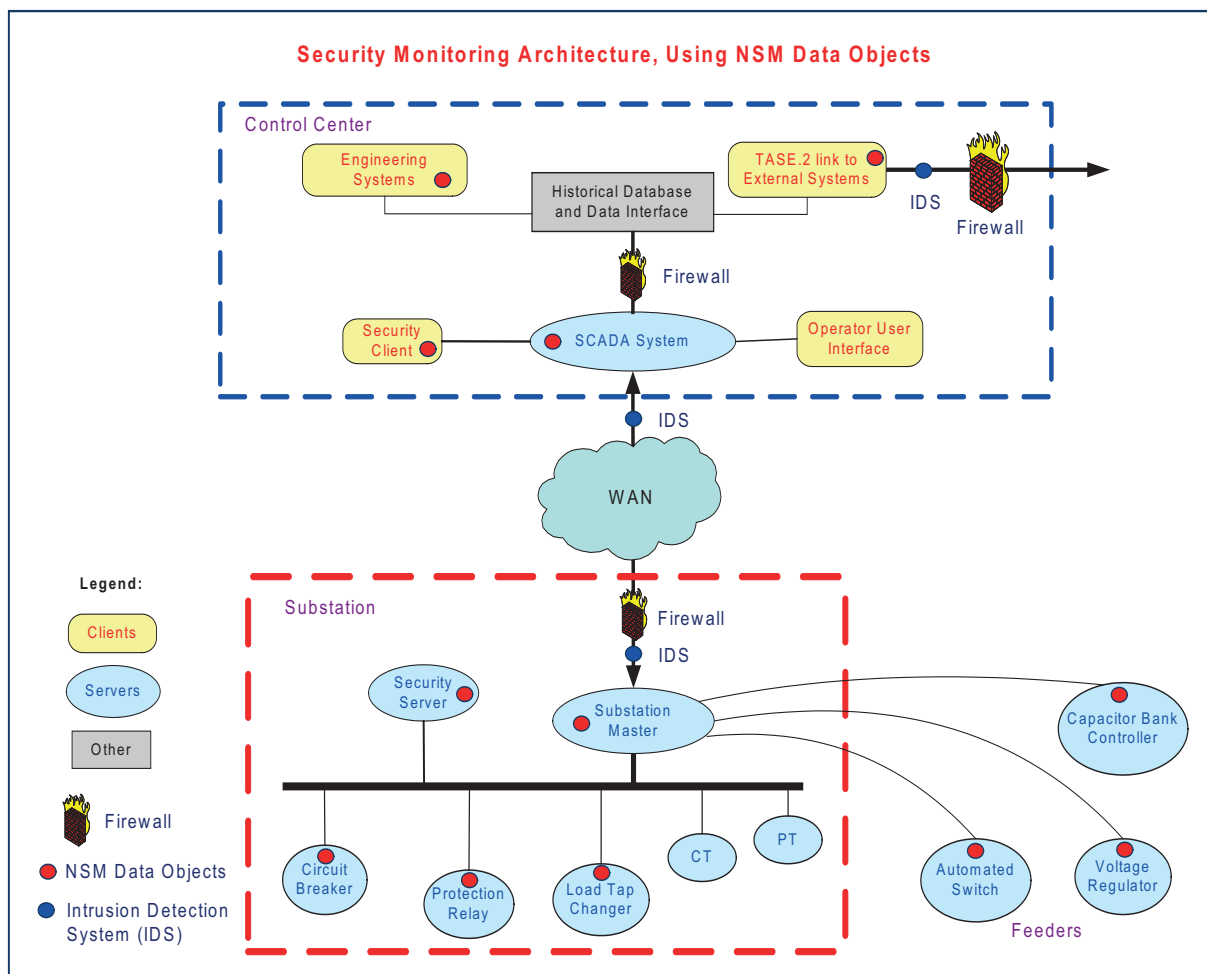


Figure 1 - Example of a power system SCADA architecture extended with NSM Data Objects

5.2 NSM Concepts

5.2.1 Simple Network Management Protocol (SNMP)

The simple network management protocol (SNMP) was developed by the IETF as the protocol for transmitting Management Information Base (MIB) objects over the Internet. A Management Information Base (MIB) is a database defining hierarchical data objects, with each object addressed through an object identifier (OID). These data objects are used to define which information may be used to monitor and manage a network infrastructure. MIB objects are specified representing the state of different equipment, applications, and systems.

Many systems use SNMP over internal communication networks as well. Due to SNMP its popularity SNMP is the preferred protocol to transmit MIBs. However, other protocols may be used as well.

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.

Although some existing MIB objects are generic enough for typical network equipment and should be used by the power industry, many specialized MIB objects are needed to

represent some of the very specialized equipment and special environments deployed in power system operations.

5.2.2 ISO NSM categories

Network management aspects have been organized by ISO into 5 areas:

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

Of these 5 areas, only accounting management is not relevant to this standard. The other 4 areas are either directly or indirectly involved in power operation security. For instance, if an equipment failure or a careless parameter change causes a degradation of performance, then the reliability of the power system operations may be affected; or a change in the network configuration could result in a single point of failure that is not recognized until that failure occurs; or an undetected intrusion may cause the violation of transmission time constraints required by time-sensitive data exchanges.

5.2.3 NSM “data objects” for power system operations

The NSM “data objects” identified in this standard fill the gap between the existing 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) as well as SNMP.

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

5.3 Communication network management

5.3.1 Network configuration

Typical network management involves monitoring and controlling the communication network and its configuration. Most vendors of enterprise-level network equipment provide some degree of control. Wherever these control capabilities are available in power system operations, these capabilities should be used. 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. Depending on the implementation and configuration, this information can be “downloaded” from another node 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 cycle (on/off) commands to network equipment.
- Reset command to network equipment.
- Establishing primary and, optionally, secondary paths to each end device.



- Switching commands to network equipment for changing paths to devices.
- Setting or updating the access control list and RBAC rules.
- Setting parameters and sequences for automated network actions in response to event, such as reconfiguration of the communications network upon equipment failure.
- Specific mappings towards monitoring and control protocol may not include some of the above data in order to avoid duplicated and possibly conflicting configurations.

5.3.2 Network backup

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;
- logging of status and times of all failovers and use of backup equipment.

5.3.3 Communications failures and degradation

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 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.

5.4 Communication protocols

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.

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 disruptions such as loss or degradation of connectivity;
- detecting invalid network accesses;
- detecting invalid application object accesses/operations;
- 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;
 - counting number of lost messages;
- providing audit logs and records;
- detecting application protocol timeouts;
- detecting invalid sequence numbers of application messages.

5.5 End systems management

Monitoring of power 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.

Since the power 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;
- 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.

5.6 Intrusion detection systems (IDS)

5.6.1 IDS guidelines

Intrusion detection systems monitor network communication packets and detect any packet that is foreign in a particular network. IDS should warn operators as soon as an intrusion is detected and should inform what kind of vulnerability is being exploited.

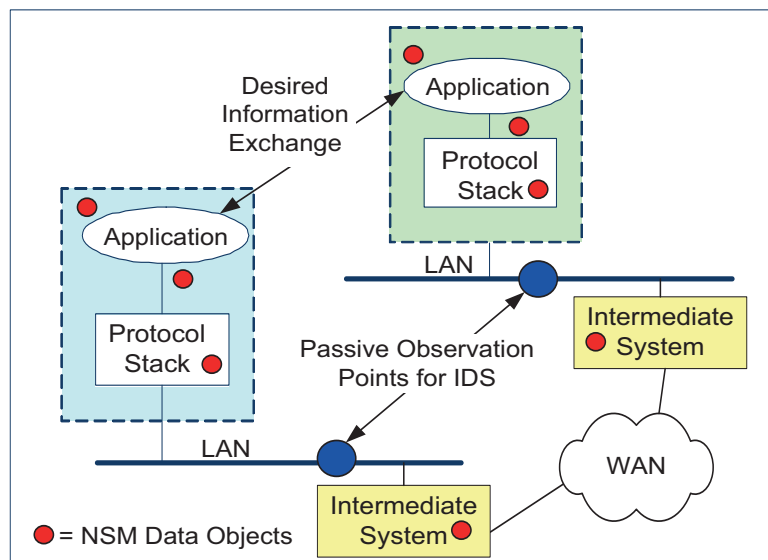


Figure 2 - IDS Information exchange between applications:
generic communication topology

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;

- 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.

5.6.2 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 2 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 2). 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.

5.6.3 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 manager”, 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.

329 A security provider would manage the NSM data objects, possibly setting appropriate
330 thresholds, limits, and other parameters in order to fine-tune the response to more closely fit
331 each power system operational environment. Upon the detection of an anomaly, the NSM
332 data would be sent to the security manager for additional analysis.

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

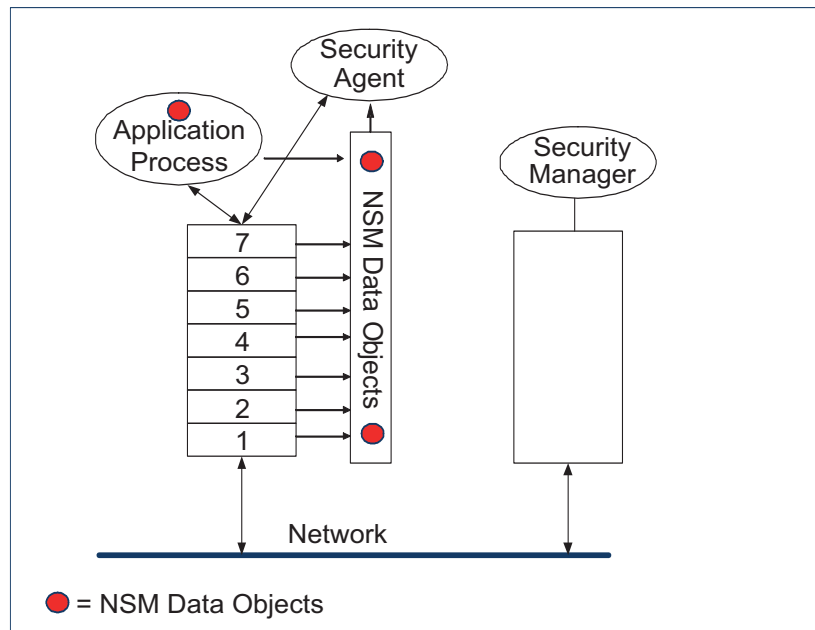


Figure 3 - Active security monitoring architecture with NSM data objects

5.7 End-to-end security

5.7.1 End-to-end security concepts

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.

End-to-end security entails a much larger scope than just the authentication of users and the securing of the 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 62351 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.

5.7.2 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 5, the entire information infrastructure must be made secure and reliable in order to provide security and reliability of power system operations. Figure 5 shows the management of both the power system infrastructure and the information infrastructure.

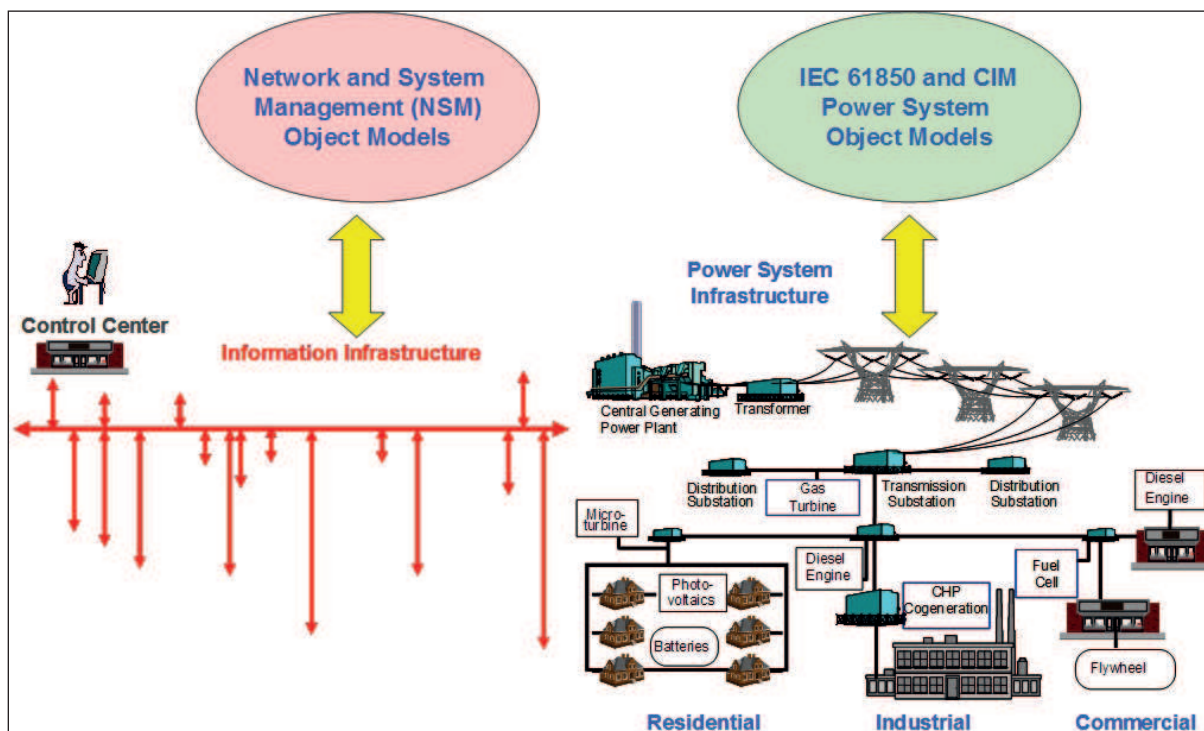


Figure 4 - Comparison of NSM data objects with IEC 61850 objects

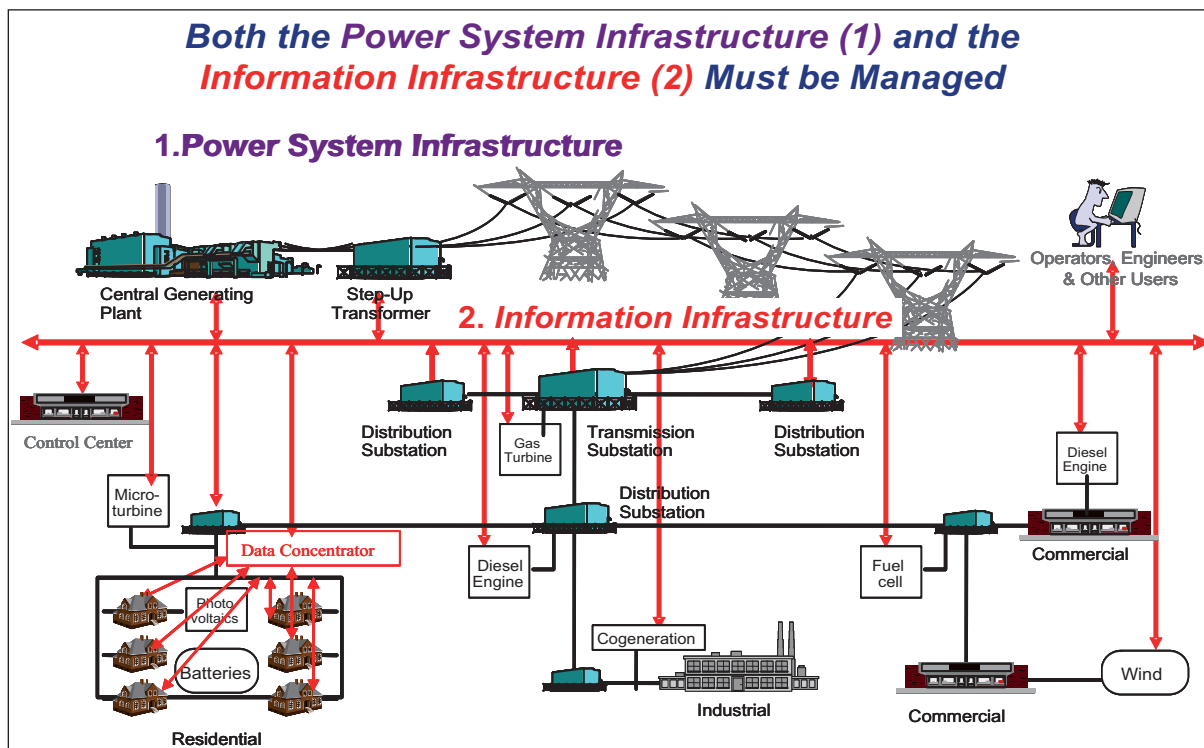


Figure 5 - Management of both the power system infrastructure

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” 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.

5.8 NSM requirements : detection functions

5.8.1 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;

5.8.2 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:

- 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.
- 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.
- 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;

- 462 • exceeding CPU load limits;
- 463 • exceeding memory usage limits;

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

467 **5.8.3 Detecting invalid buffer access DoS attacks**

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

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

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

477 **5.8.4 Detecting tampered/Malformed PDUs**

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

485 The NSM data objects in this category include:

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

489 **5.8.5 Detecting physical access disruption**

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

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

- 495 • loss of power to equipment and time of loss;
- 496 • media disconnected and time of disconnect;
- 497 • power restored to equipment and time of restoration;
- 498 • media re-connected and time of reconnection.

499 **5.8.6 Detecting invalid network access**

500 Firewalls are designed to prevent invalid access to networks, particularly through the use of
501 access control lists which permit only authorized IP addresses to pass through the firewall.
502 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).

5.8.7 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 across all communications and end systems.

5.9 Abstract Object and Agent UML description

5.9.1 Purpose of UML

The NSM object definition in this standard are intended to be defined as “abstract” with the goal to allow the mapping of the objects toward different NSM protocols. For this reason the object are defined using UML (Unified Modelling Language).

UML is a flexible and powerful tool for object modelling and it is already widely used within IEC for the development of several standards (e.g. CIM and IEC 61850).

UML supports the abstract description of the objects and at the same time provides a complete collection of the information needed for the mapping towards specific protocols. In other words the semantics of Abstract Object can be defined using UML description tools, and each Object is described as a UML Class or Class Attribute.

UML can be translated then into different NSM real protocols notations (e.g. SNMP MIBs) through the adoption of an appropriate semantics translator that will produce the specific protocol objects semantics according with the original UML description.

This standard introduces the IEC 62351-7 UML Abstract Objects Model that includes:

- the description of the Abstract Types as a common list of object (UML classes) that can be reused inside different monitoring agent.
- the description of the Base Types proper of SNMP mapping.
- the description of Abstract Classes providing attributes common to several Agent definition classes.
- Specific Monitoring Agents/Subagents which are described as packages of Classes each containing a set of attributes that can be specific of the Agent or inherited from an Abstract Classes.

5.9.2 Abstract Types and Base Types

The primary objective of this standard is to define and describe the NSM objects using an Abstract notation that can allow the translation of those objects and their semantics into specific NSM protocols objects. A further objective is the translation of those objects into SNMP MIBs objects. This standard needs therefore the description of Abstract Types not constrained by the limits and notation of SNMP while still providing a set of Base Types that are compatible with the SNMP standard types.

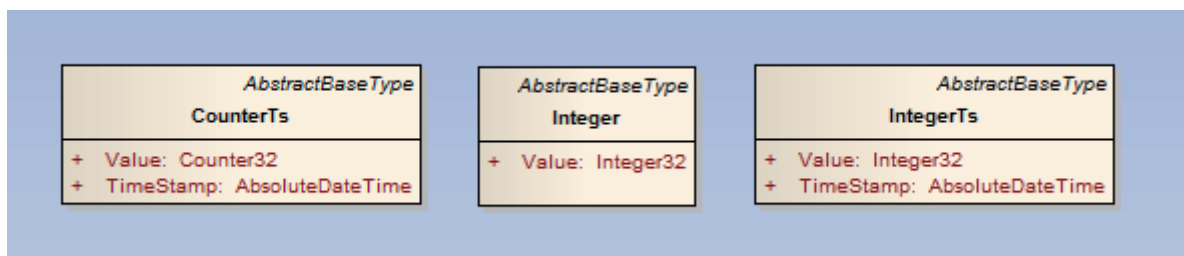


Figure 6 - Abstract Types

Figure 6 - Abstract Types, depicts an example of some Abstract Types showing the difference between the Abstract Object name and the semantics of the Base types that are referenced as Class Attribute types.

Base Types Package included a set of Classes that respect the same naming convention of SNMP types, in order to allow the automated translation of UML attributes types into SNMP types. However, the Attribute Type that is used inside the model classes that describe the

Monitoring Agents does not reference the Base Type directly. Instead, the Agent Classes attributes reference the Abstract Types. Each Abstract Type refers to Base types indirectly. This allows a decoupling between the Abstract Agent classes and the SNMP translation, thus permitting future translations to different native types of other different protocols.

Each Abstract Type is represented in the UML model through a specific Class declaration. The name of the class is intended to be almost self-explanatory but the class description also includes an explanation of the type semantics. For instance, when an Abstract Type class has the “Ts” suffix this mean that the Abstract Object will actually provide a “Value” of the Object and a “Timestamp” to be set simultaneously with the related value. For instance a counter object value makes more sense when the last time when the counter has been incremented is also well-known. This can be considered as implicit but the choice was instead to make it explicit in the class semantics.

The Package “BaseTypes” contains the definition of the type used in the definition of the Abstract type UML classes attributes.

5.9.3 Enumerated Types

The Enumerated Types package provides the definition of enumerated values used for the Abstract Agent Object Attributes. Figure 7, depicts an example of the Enumerated Type declaration with the two types of “value only” and “Value and Timestamp” declaration.

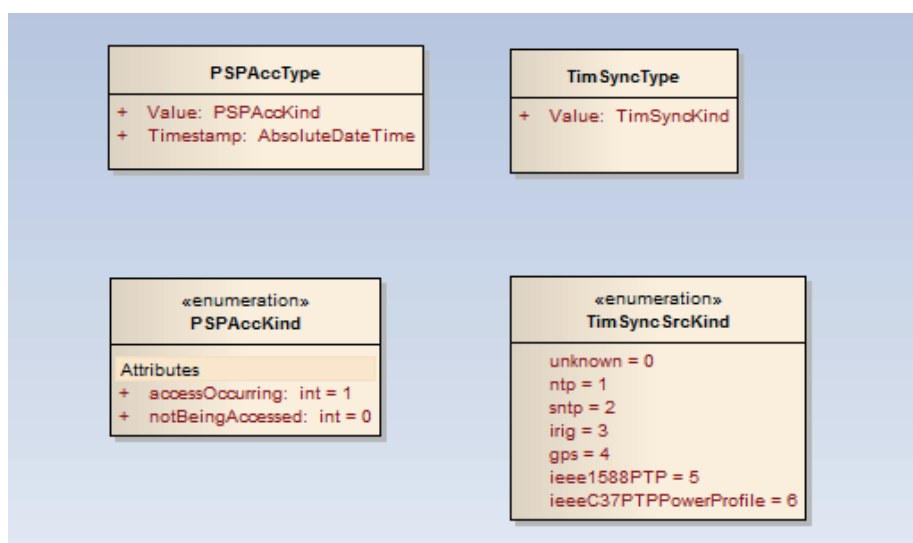


Figure 7 - Enumerated Types

The concept of Enumerated Types declaration is almost the same of the one adopted for Abstract Objects, although not all Enumerated Types require a Timestamp. Therefore the attribute of an Enumerated Type may include both a Value and a Timestamp or may include only a Value, In both cases, the type is declared as an “enumeration” stereotype class.

5.9.4 Abstract Agents

The concept of an Agent is related to the procedure of Abstract Types deployment within a real IED, and is connected also to the architecture of the NSM software that actually runs on this device. The type of Agent depends on the adopted NSM protocol.

616 The concept of Agent/Subagent architecture (and the “Agent/subagent” terminology) arises
617 from the terminology of the SNMP NSM protocol. This standard uses this Agent/Subagent
618 concept and the related architecture as an Abstract idea.

619 An Agent/Subagent for the purposes of this standard can be summarized with the concept of
620 a set of Abstract Objects that are related to a homogeneous environment of NSM Objects
621 inside the IED. Each of those homogenous objects values sets are expected to be populated
622 by an independent software component, called the subagent, even if for some NSM
623 protocols (like SNMP) only one of these agents could be in charge of the communication with
624 central NSM system.

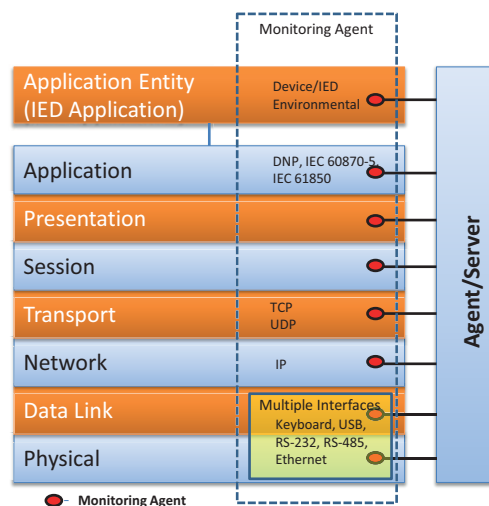
625 This architecture thus allows the activation of specific subagents of an NSM object set only
626 when those subagents are actually useful.

627 The homogenous set of objects include the following:

- 628 • **Environmental Agent:** device Physical and power security and health
- 629 • **Device Agent:** general device status (e.g. CPU, Storage, Certificate status)
- 630 • **Application Protocol Agents:** application protocols Statistics, status and alarms
- 631 • **Interfaces Agent:** The interfaces that need to be monitored are keyboards, USB,
632 Serial, and Ethernet
- 633 • **Clocks Agent:** Status and health of clock synch system.

634 Each agent/subagent is responsible for updating Values and related Timestamps of its own
635 instances of each Abstract Object.

636



637

638

Figure 8 - Subagents

639

640 Depending on the translation on specific NMS protocol, the communication towards the
641 central NMS is delegated to one particular Agent that acts as a communication mediator for
642 the other agents that in this case act as subagents (this is the case of SNMP). Figure 8
643 provide the view of the agent/subagent hierarchy.

644 The Agent/Subagent structure is implemented using UML packages. Within each package
645 the classes describe the following basic entities:

- UML classes having “nsmAgent” stereotype: this are the classes which contain as attributes the NSM Abstract Object
- The Attributes of nsmAgent Classes, defined with a set of possible stereotypes which express the conceptual role of the Attribute
- UML classes having “nsmEvent” stereotype: these are the classes which contain, as attributes, the object to be notified in case of event.

Each package can also host special common classes that contain the attributes of common use among several agents. An Agent can therefore inherit attributes from these common classes, avoiding attribute declaration duplication.

In Figure 9, the main agent Environmental is presented. Please note that a subsidiary nsmAgent PSUPEntry class is represented next to Environmental class, and PSUPEntry is also the Attribute Type of PSUP Attribute. PSUP Attribute also show 1..* multiplicity.

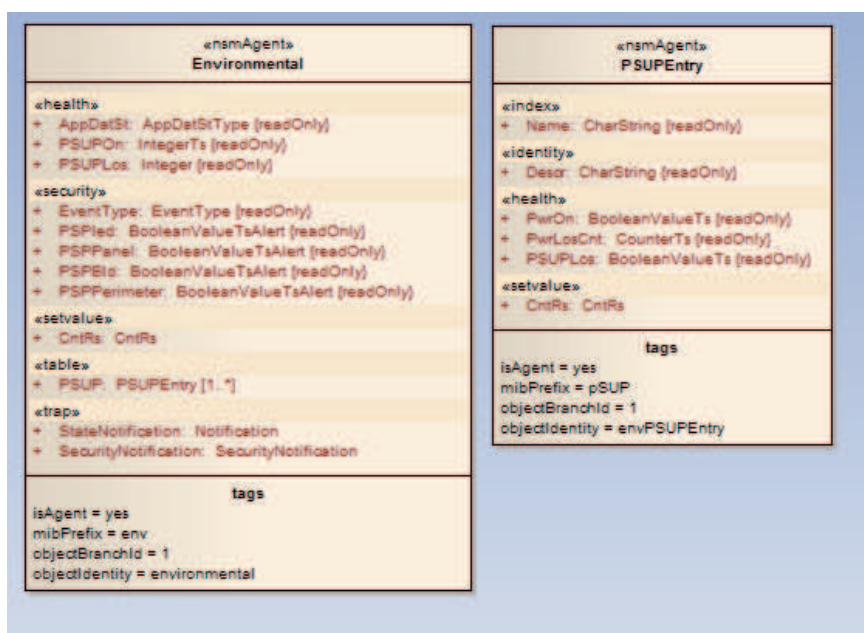


Figure 9 - Agent

This kind of notation is always used in this UML model when a set of Attributes must be supported in multiple instances (like in this case the Power Supply) and each instance must have its own set of values.

As depicted in Figure 10 an “nsmEvent” stereotype is declared. This is the stereotype that allows the declaration of a special class that includes the objects to be notified when a predefined event occurs.

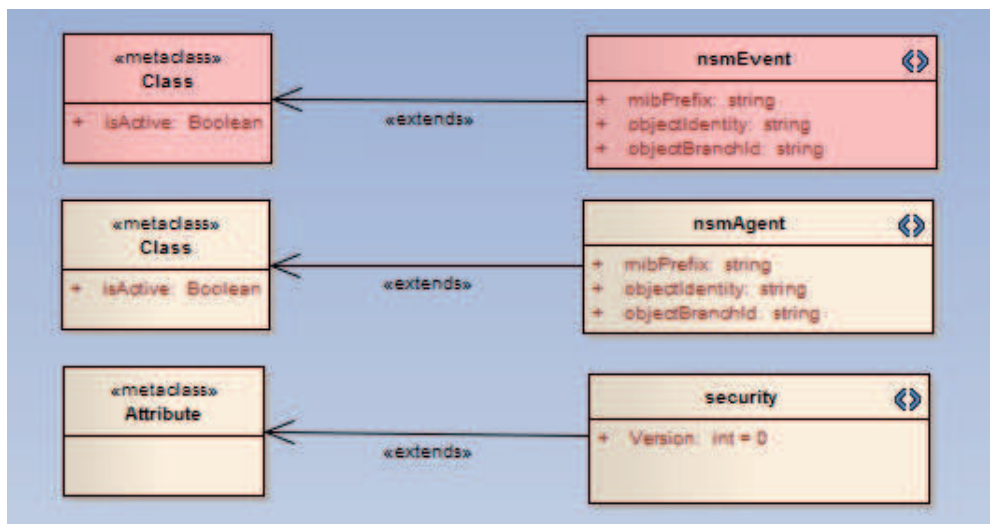


Figure 10 - Model Stereotypes

The nsmAgent stereotype declaration allow the use of an additional tool that provide for each class or attribute some additional information that are not strictly related to the Abstract model but are instead unavoidable when the model objects must be translated into SNMP MIBs (or also in future towards different protocols).

We have therefore some stereotypes attributes that will be represented as “tags” for nsmAgent classes and for the related attributes.

5.9.5 Unsolicited Event Notification

A model for spontaneous NSM Event notification is included in the design of this standard UML model. The event recognition is a local function of the IED. One or more NSM Abstract Classes declare the object to be notified in an attribute list. This set of objects is defined in UML model in the “nsmEvent” classes.

5.10 Abstract Object UML translation towards SNMP

5.10.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) was developed by the IETF as protocol of level 7 OSI, in order to support the activity of configuration, monitoring and management of devices connected over a network.

The SNMP-management infrastructure includes three main components: managed devices, agents, and network-management systems (NMSs).

A managed device is a node inside the network that incorporates an SNMP agent and is part of a managed network. Inside a managed device, information is collected, stored and accessed by Central NMSs using the SNMP protocol. Managed devices (or network elements) can be, for instance, routers, switches and bridges, but also IEDs and local and remote SCADA.

An agent is a software module that resides inside a managed device. This module is in charge of the exposure of the information through the use of SNMP protocol using a structured data format that is called a MIB (Management Information Base) (see next clause).. The agent has local knowledge of management information and must expose that information into a form compatible with SNMP.

An SNMP agent can be actually present in a single Managed Device in multiple instances, implemented as an Agent-Subagent architecture, with a main Agent that is in charge of the communication with NMSs (many NMS can exist inside the managed network) and the subagents that are specialized in the collection of specific part of information. This approach allow an SNMP agent modular implementation with agent also provided by independent manufacturer.

The protocol allows not only information reading but also permits active management tasks, for instance the modification of the variables exposed by the agent.

5.10.2 Management information bases (MIBs)

The variables accessible via SNMP are organized in hierarchies. The Management Information Bases (MIBs) are the entities that describe such hierarchies, together with the metadata such as type and description of the variable.

Inside a MIB there is the description of the structure of the management data of a device subsystem, organized in a hierarchical namespace and named object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

MIBs use the notation defined by Structure of Management Information Version 2 (SMIPv2, RFC 2578), that is a subset of ASN.1. Note that SMIPv2 is only a subset and not a full ASN.1 notation. Therefore some constraints in the naming and structuring of the hierarchy and object reuse apply.

In SMIPv2 an OID uniquely identifies a managed object in the MIB hierarchy. The top-level MIB object IDs belong to different standard organizations, while lower-level object IDs are allocated by associated organizations.

The Internet Assigned Numbers Authority (IANA), among the other coordination activity, is responsible also for the assignment of the Private Enterprise Numbers.

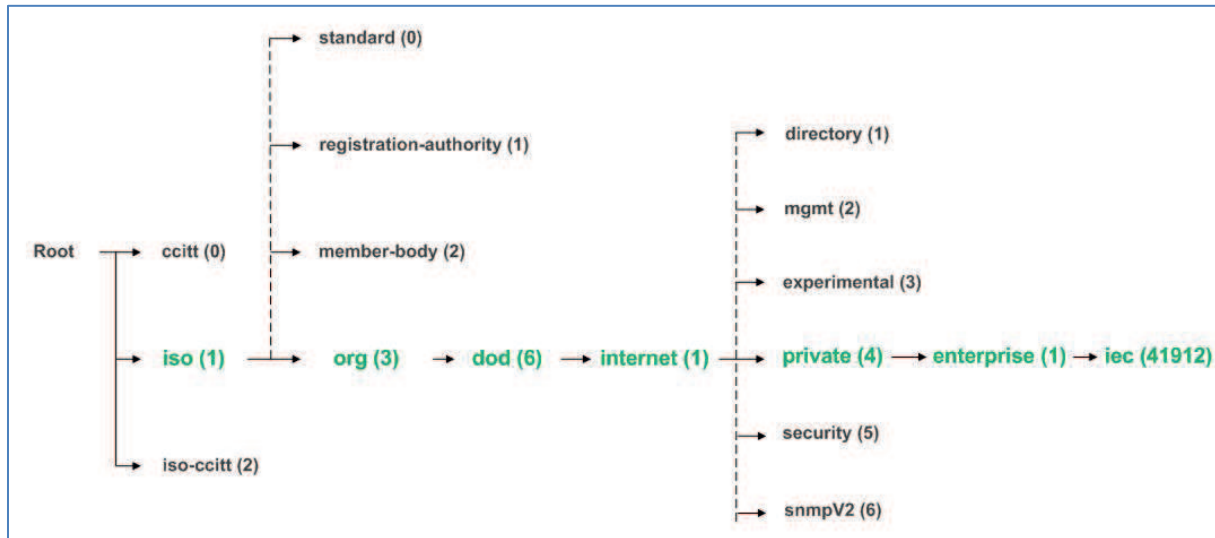


Figure 11 - MIB hierarchy

Vendors can define private branches that include managed objects for their own products. MIBs that have not been standardized typically are positioned in the experimental branch.

The IANA Private Enterprise Number (PEN) for IEC is 41912, under the enterprise branch. The full path is: **iso.org.dod.internet.private.enterprise.iec (1.3.6.1.4.1.41912)**.

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.

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.

This document covers the definition of the MIBs needed to manage the specific information related to IEDs not already covered by an RFC defined MIBs.

5.11 SNMP mapping of UML model Objects

The translation of the object defined inside this standard and their semantics into SNMP object and semantics is carried out adopting the following translation rules:

- The UML model package hierarchy start from the IEC root, and each nested package maps into a new level of SNMP OID hierarchy. This produces an OIDs structure that is “parallel” to the UML module Package structure. Only the Packages that provide the “objectIdentity” and “objectBranchId” tags are considered for the structure generation process:
 - “objectIdentity” tag will be the symbolic name of the branch
 - “objectBranchId” tag will be the OID branch number.
- The Enumerated Values package is used for the production of the corresponding SNMP MIB enumerations. In order to be recognized by an automatic translator this package includes a tag named “isEnumeration” set to “yes”
- The Abstract Types Package includes a set of Classes. Each class provides one or both the attributes:

- “Value”: the actual Abstract object Value referring the actual type, selected among the Base Types and used for SNMP object type assignment.
- “TimeStamp”: the object that is generated together with the “Value” object, that refers to the timestamp of the last Value set.
- The Packages exposing the “isAgent” tag set to “yes” are to be considered within the SNMP objects production process.
- “nsmAgent” stereotype Class are intended to be selected for SNMP object generation process. Each class attribute automatically translates into one or more SNMP objects depending on the Abstract Type declaration. Attributes that are defined as constant are translated into a read-only SNMP object.
- “nsmEvent” stereotype Class are selected for SNMP trap object generation process. Each Class attribute is automatically translated into one or more SNMP trap objects depending on the Abstract Type declaration.

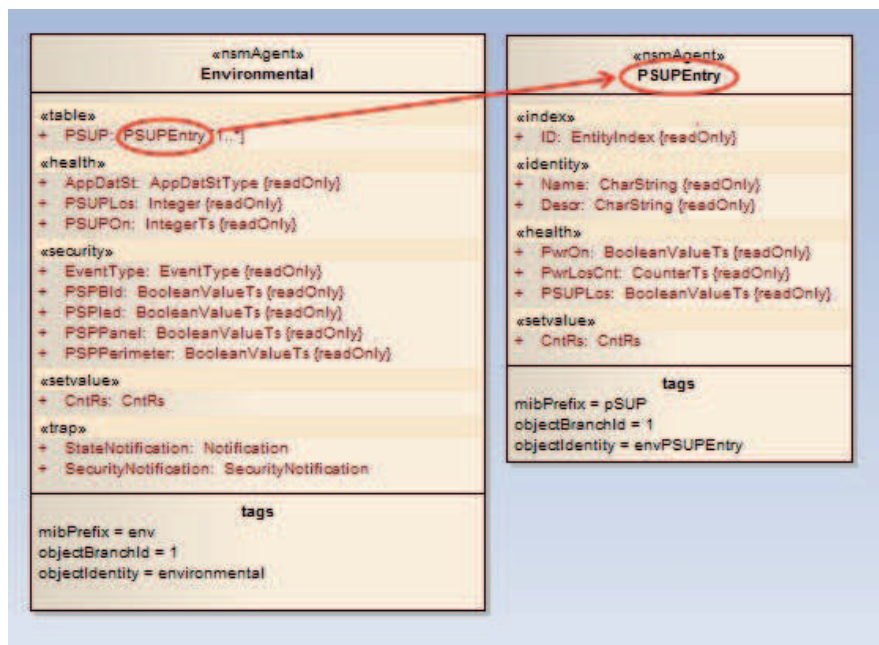


Figure 12 - SNMP Table

The following rules apply to the translation of each Agent Class into MIB objects:

- Multiplicity of Class Attribute higher than “x..1” (i.e. 0..*) produces a SNMP table reference. As depicted in Figure 12 the UML type of this attribute is actually the Class name which provides the Attributes to be included in SNMP table sequence as tabular objects.
- Class Attribute names are translated into SNMP object names using the mibPrefix tag value as a prefix. This avoids the SNMP MIB SMIv2 constrain that does not allow replication of the same SNMP object name in several object descriptions.
- The SNMP object is generated, including all the inherited Attributes.
- The SNMP object OID is automatically generated in sequence within the same Agent Class.
- Each Attribute owns a “Version” tag. This Version tag is provided in order to allow the future extension of this UML model to add new Attributes, giving evidence that the additional attributes belong to a more recent version. This allows the automatic translation of the additional attributes as objects at the end of the

790 existing list of SNMP MIB object of the same branch without affecting the SNMP
791 OIDs mapping of older MIB objects.
792

793 **5.12 SNMP transport and Security**

794
795 Since the beginning and for a long time Security has been a weakness of SNMP. SNMP
796 Versions 1 and 2 actually do not implement a real authentication mechanism because they
797 rely on nothing more than a shared password (community string) that is sent in clear text
798 between a manager and agent.

799 SNMP versions 1 and 2c are subject to packet sniffing of the clear text community string from
800 the network traffic, because they do not implement encryption.

801 SNMPv3 introduced the authentication feature because message includes security
802 parameters which are encoded as an octet string. SNMPv3 provides the following security
803 features:

- 804 • Confidentiality using encryption of packets.
- 805 • Integrity of messages in transit including an optional packet replay protection.
- 806 • Authentication to verify that the message is from a known and authorized source.
- 807 • Confidentiality can both be provided through the use of SNMPv3 or trusted networks
808 established through the use of VPNs.

809 All versions of SNMP are subject to brute force and dictionary attacks for guessing the
810 community strings, authentication strings, authentication keys, encryption strings, or
811 encryption keys, because they do not implement a challenge-response handshake.

812 Although SNMP works over TCP and other protocols, it is most commonly used over UDP
813 that is connectionless and vulnerable to IP spoofing attacks. Thus, all versions are subject to
814 bypassing device access lists that might have been implemented to restrict SNMP access,
815 though SNMPv3's other security mechanisms should prevent a successful attack.

816 SNMP's powerful configuration (write) capabilities are not being fully utilized by many
817 vendors, partly because of a lack of security in SNMP versions before SNMPv3 and partly
818 because many devices simply are not capable of being configured via individual MIB object
819 changes.