



BSI Standards Publication

Power systems management and associated information exchange - Data and communications security

Part 7: Network and System Management (NSM) data object models

National foreword

This British Standard is the UK implementation of EN 62351-7:2017. It is identical to IEC 62351-7:2017. It supersedes DD IEC/TS 62351-7:2010, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 89558 6

ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

**Power systems management and associated information
exchange - Data and communications security -
Part 7: Network and System Management (NSM) data object
models
(IEC 62351-7:2017)**

Gestion des systèmes d'alimentation et échange
d'informations associées - Sécurité des données et des
communications - Partie 7: Modèles d'objets de données
pour la gestion des réseaux et systèmes (NSM)
(IEC 62351-7:2017)

Datenmodelle, Schnittstellen und Informationsaustausch für
Planung und Betrieb von Energieversorgungsunternehmen
- Daten- und Kommunikationssicherheit -
Teil 7: Netzwerk und System-Management (NSM) Daten-
Objekt-Modelle
(IEC 62351-7:2017)

This European Standard was approved by CENELEC on 2017-08-22. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 57/1857/FDIS, future edition 1 of IEC 62351-7, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62351-7:2017.

The following dates are fixed:

- latest date by which the document has to be (dop) 2018-06-15
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-12-15
standards conflicting with the
document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 62351-7:2017 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61850-7-2	NOTE	Harmonized as EN 61850-7-2.
IEC 61850-7-4	NOTE	Harmonized as EN 61850-7-4.
IEC 61850-8-1	NOTE	Harmonized as EN 61850-8-1.
IEC 61850-9-2	NOTE	Harmonized as EN 61850-9-2.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC/TS 62351-1	-	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues	-	-
IEC/TS 62351-2	-	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
IEC 62351-3	-	Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP	EN 62351-3	-
IEC 62351-4 ¹	-	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS	prEN 62351-4 ²	-
IEC/TS 62351-5	-	Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives	-	-
IEC/TS 62351-8	-	Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control	-	-
IEC 62351-9	-	Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment	EN 62351-9	-

¹ Under preparation. Stage at the time of publication: IEC CDV 62351-4:2017.

² Under preparation. Stage at the time of publication: prEN 62351-4:2017.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEEE 754	2008	IEEE Standard for Binary Floating-Point Arithmetic	-	-
IETF RFC 2578	1999	Structure of Management Information Version 2 (SMIv2), April 1999, http://tools.ietf.org/html/rfc2578	-	-
IETF RFC 3410	2002	Introduction and Applicability Statements for Internet Standard Management Framework, December 2002, http://tools.ietf.org/rfc/rfc3410	-	-
IETF RFC 3414	2002	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002, http://tools.ietf.org/rfc/rfc3414	-	-
IETF RFC 3826	2004	The Advanced Encryption Standard (AES) - Cipher Algorithm in the SNMP User-based Security Model, June 2004, http://www.rfc-editor.org/rfc/rfc3826	-	-
IETF RFC 4022	2005	Management Information Base for the Transmission Control Protocol (TCP), March 2005, http://tools.ietf.org/html/rfc4022	-	-
IETF RFC 4113	2005	Management Information Base for the User-Datagram Protocol (UDP), June 2005, http://tools.ietf.org/html/rfc4113	-	-
IETF RFC 4292	2006	IP Forwarding Table MIB, April 2006, http://www.rfc-editor.org/rfc/rfc4292	-	-
IETF RFC 4293	2006	Management Information Base for the Internet Protocol (IP), April 2006, http://tools.ietf.org/rfc/rfc4293	-	-
IETF RFC 4898	2007	TCP Extended Statistics MIB, May 2007, http://tools.ietf.org/rfc/rfc4898	-	-
IETF RFC 5132	2007	IP Multicast MIB, December 2007, http://tools.ietf.org/rfc/rfc5132	-	-
IETF RFC 5905	2010	Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010, http://tools.ietf.org/rfc/rfc5905	-	-
IETF RFC 5590	2009	Transport Subsystem for the Simple Network Management Protocol (SNMP), June 2009, http://tools.ietf.org/rfc/rfc5590	-	-
IETF RFC 5591	2009	Transport Security Model for the Simple Network Management Protocol (SNMP), June 2009, http://tools.ietf.org/rfc/rfc5591	-	-
IETF RFC 5592	2009	Secure Shell Transport Model for the Simple Network Management Protocol (SNMP), June 2009, http://www.rfc-editor.org/rfc/rfc5592	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IETF RFC 5953	2010	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), August 2010, http://www.rfc-editor.org/rfc/rfc5953	-	-
IETF RFC 6347	2012	Datagram Transport Layer Security Version 1.2, January 2012, http://tools.ietf.org/rfc/rfc6347	-	-
IETF RFC 6353	2011	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), July 2011, http://tools.ietf.org/rfc/rfc6353	-	-
IETF RFC 7860	2016	HMAC-SHA-2, Authentication Protocols in User-Based Security Model (USM) for SNMPv3, April 2016, http://tools.ietf.org/rfc/rfc7860	-	-

This page deliberately left blank

CONTENTS

FOREWORD.....	8
1 Scope	10
2 Normative references	10
3 Terms and definitions	12
4 Abbreviated terms and acronyms.....	13
5 Overview of Network and System Management (NSM)	14
5.1 Objectives.....	14
5.2 NSM concepts.....	15
5.2.1 Simple Network Management Protocol (SNMP)	15
5.2.2 ISO NSM categories	15
5.2.3 NSM “data objects” for power system operations	16
5.2.4 Other NSM protocols	16
5.3 Communication network management.....	16
5.3.1 Network configuration	16
5.3.2 Network backup.....	17
5.3.3 Communications failures and degradation	17
5.4 Communication protocols.....	18
5.5 End systems management	18
5.6 Intrusion detection systems (IDS)	19
5.6.1 IDS guidelines	19
5.6.2 IDS: Passive observation techniques	20
5.6.3 IDS: Active security monitoring architecture with NSM data objects	20
5.7 End-to-end security.....	21
5.7.1 End-to-end security concepts.....	21
5.7.2 Role of NSM in end-to-end security	22
5.8 NSM requirements: detection functions	24
5.8.1 Detecting unauthorized access	24
5.8.2 Detecting resource exhaustion as a denial of service (DoS) attack	24
5.8.3 Detecting invalid buffer access DoS attacks	25
5.8.4 Detecting tampered/malformed PDUs	25
5.8.5 Detecting physical access disruption	25
5.8.6 Detecting invalid network access	25
5.8.7 Detecting coordinated attacks.....	26
5.9 Abstract object and agent UML descriptions.....	26
5.9.1 Purpose of UML.....	26
5.9.2 Abstract types and base types	27
5.9.3 Enumerated Types.....	28
5.9.4 Abstract agents	28
5.9.5 Unsolicited Event Notification	31
5.9.6 UML Model extension	31
5.10 Abstract Object UML translation to SNMP.....	31
5.10.1 Simple Network Management Protocol (SNMP)	31
5.10.2 Management information bases (MIBs).....	32
5.11 SNMP mapping of UML model Objects.....	33
5.12 SNMP Security.....	34
6 Abstract objects.....	36

6.1	General.....	36
6.2	Package Abstract Types	37
6.2.1	General	37
6.2.2	BooleanValue	37
6.2.3	BooleanValueTs	37
6.2.4	CounterTs.....	37
6.2.5	CntRs	38
6.2.6	Floating	38
6.2.7	FloatingTs	38
6.2.8	EntityIndex	39
6.2.9	Integer	39
6.2.10	IntegerTs	39
6.2.11	InetAddress	40
6.2.12	InetAddressType	40
6.2.13	MacAddress.....	40
6.2.14	Selector	40
6.2.15	Timestamp.....	41
6.2.16	CharString	41
6.2.17	CharStringTs	41
6.2.18	AbstractBaseType root class	41
6.2.19	AbstractAgent root class.....	42
6.3	Package EnumeratedTypes	42
6.3.1	General	42
6.3.2	AppDatStKind enumeration.....	42
6.3.3	PhyHealthKind enumeration.....	42
6.3.4	ExtKind enumeration	42
6.3.5	IntKind enumeration.....	43
6.3.6	LnkKind enumeration	43
6.3.7	PSPAccKind enumeration	43
6.3.8	ProtIdKind enumeration	43
6.3.9	EventKind enumeration.....	44
6.3.10	TimSyncIssueKind enumeration.....	44
6.3.11	SecurityProfileKind enumeration.....	45
6.3.12	TimSyncSrcKind enumeration	45
6.3.13	AppDatStType	45
6.3.14	PhyHealthType	46
6.3.15	ExtType	46
6.3.16	IntType	46
6.3.17	EventType	46
6.3.18	PSPAccType	47
6.3.19	ProtIdType.....	47
6.3.20	TimSyncIssueType	47
6.3.21	SecurityProfileType	47
6.3.22	TimSyncSrcType	48
6.3.23	LnkType	48
7	Agents.....	48
7.1	Package Overview	48
7.2	Package Environmental Agent	50
7.2.1	General	

7.2.2	Environmental	51
7.2.3	PSUPEntry	51
7.2.4	Notification	52
7.2.5	SecurityNotification.....	52
7.3	Package IED Agent.....	53
7.3.1	General	53
7.3.2	IED	54
7.3.3	CPUEnter	55
7.3.4	EXTEntry.....	56
7.3.5	STOREEntry.....	56
7.3.6	Notification	57
7.3.7	SecurityNotification.....	57
7.4	Package Application Protocols Agents	57
7.4.1	General	57
7.4.2	Package Common objects	58
7.4.3	Package IEEE 1815 and IEC 60870-5 Agent.....	59
7.4.4	Package IEC61850 Agent.....	68
7.5	Package Interfaces Agent.....	87
7.5.1	General	87
7.5.2	Interface	88
7.5.3	Interfaces	88
7.5.4	ETHEntry.....	90
7.5.5	KEYEntry.....	90
7.5.6	SEREntry.....	91
7.5.7	ALGEntry.....	91
7.5.8	USBEntry.....	92
7.5.9	Notification	92
7.6	Package Clocks Agent	93
7.6.1	General	93
7.6.2	Clock	93
7.6.3	ClockEntry.....	94
7.6.4	SecurityNotification.....	95
7.7	Network and Transport Agents	95
7.7.1	TCP.....	95
7.7.2	User Datagram Protocol (UDP).....	95
7.7.3	IP	95
8	SNMP security.....	96
9	Secured time synchronization	96
Annex A (normative)	SNMP MIB Mapping	97
Annex B (informative)	Mapping of relevant IEC 61850 Objects.....	229
Bibliography.....		230

Figure 1 – Example of a power system SCADA architecture extended with NSM Data Objects 15

Figure 2 – IDS Information exchange between applications: generic communication topology..... 19

Figure 3 – Active security monitoring architecture with NSM data objects 21

Figure 4 – Comparison of NSM data objects with IEC 61850 objects..... 23

Figure 5 – Management of both the power system infrastructure and the information infrastructure	23
Figure 6 – Abstract types	27
Figure 7 – Enumerated types	28
Figure 8 – Subagents	29
Figure 9 – Environmental agent	30
Figure 10 – Model stereotypes	30
Figure 11 – Object identifier structure	32
Figure 12 – SNMP table	34
Figure 13 – SNMP RFCs map and security	35
Figure 14 – SNMP Entity	36
Figure 15 – Class diagram Overview::Part7 Classes Overview	49
Figure 16 – Class diagram Environmental Agent::Environmental	50
Figure 17 – Class diagram IED Agent::IED	53
Figure 18 – Class diagram Common objects::Application Protocol common objects	58
Figure 19 – Class diagram IEEE 1815 and IEC 60870-5 Agent::IEEE 1815 and IEC 60870 Agent Relationships	60
Figure 20 – Class diagram ACSI::ACSI	69
Figure 21 – Class diagram MMS::MMS	71
Figure 22 – Class diagram SV and GSE common objects::SV and GSE common objects	76
Figure 23 – Class diagram SV::SV	78
Figure 24 – Class diagram GSE::GSE	82
Figure 25 – Class diagram Interfaces Agent::Interfaces	87
Figure 26 – Class diagram Clocks Agent::Clocks Agent	93
Table 1 – Attributes of Abstract Types::BooleanValue	37
Table 2 – Attributes of Abstract Types::BooleanValueTs	37
Table 3 – Attributes of Abstract Types::CounterTs	38
Table 4 – Attributes of Abstract Types::CntRs	38
Table 5 – Attributes of Abstract Types::Floating	38
Table 6 – Attributes of Abstract Types::FloatingTs	39
Table 7 – Attributes of Abstract Types::EntityIndex	39
Table 8 – Attributes of Abstract Types::Integer	39
Table 9 – Attributes of Abstract Types::IntegerTs	39
Table 10 – Attributes of Abstract Types::InetAddress	40
Table 11 – Attributes of Abstract Types::InetAddressType	40
Table 12 – Attributes of Abstract Types::MacAddress	40
Table 13 – Attributes of Abstract Types::Selector	41
Table 14 – Attributes of Abstract Types::Timestamp	41
Table 15 – Attributes of Abstract Types::CharString	41
Table 16 – Attributes of Abstract Types::CharStringTs	41
Table 17 – Literals of EnumeratedTypes::AppDatStKind	42
Table 18 – Literals of EnumeratedTypes::PhyHealthKind	

Table 19 – Literals of EnumeratedTypes::ExtKind	43
Table 20 – Literals of EnumeratedTypes::IntKind	43
Table 21 – Literals of EnumeratedTypes::LnkKind	43
Table 22 – Literals of EnumeratedTypes::PSPAccKind	43
Table 23 – Literals of EnumeratedTypes::ProtIdKind	44
Table 24 – Literals of EnumeratedTypes::EventKind	44
Table 25 – Literals of EnumeratedTypes::TimSyncIssueKind	44
Table 26 – Literals of EnumeratedTypes::SecurityProfileKind	45
Table 27 – Literals of EnumeratedTypes::TimSyncSrcKind	45
Table 28 – Attributes of EnumeratedTypes::AppDatStType	46
Table 29 – Attributes of EnumeratedTypes::PhyHealthType	46
Table 30 – Attributes of EnumeratedTypes::ExtType	46
Table 31 – Attributes of EnumeratedTypes::IntType	46
Table 32 – Attributes of EnumeratedTypes::EventType	47
Table 33 – Attributes of EnumeratedTypes::PSPAccType	47
Table 34 – Attributes of EnumeratedTypes::ProtIdType	47
Table 35 – Attributes of EnumeratedTypes::TimSyncIssueType	47
Table 36 – Attributes of EnumeratedTypes::SecurityProfileType	48
Table 37 – Attributes of EnumeratedTypes::TimSyncSrcType	48
Table 38 – Attributes of EnumeratedTypes::LnkType	48
Table 39 – Attributes of Environmental Agent::Environmental	51
Table 40 – Attributes of Environmental Agent::PSUPEntry	51
Table 41 – Attributes of Environmental Agent::Notification	52
Table 42 – Attributes of Environmental Agent::SecurityNotification	52
Table 43 – Attributes of IED Agent::IED	54
Table 44 – Attributes of IED Agent::CPUEntry	55
Table 45 – Attributes of IED Agent::EXTEntry	56
Table 46 – Attributes of IED Agent::STOREEntry	56
Table 47 – Attributes of IED Agent::Notification	57
Table 48 – Attributes of IED Agent::SecurityNotification	57
Table 49 – Attributes of Common objects::CommonProtocollInfo	58
Table 50 – Attributes of IEEE 1815 and IEC 60870-5 Agent::60870andDNPProtocollInfo	61
Table 51 – Attributes of IEEE 1815 and IEC 60870-5 Agent::Association	62
Table 52 – Attributes of IEEE 1815 and IEC 60870-5 Agent::Summary	64
Table 53 – Attributes of IEEE 1815 and IEC 60870-5 Agent::60870andDNPSecurityNotification	65
Table 54 – Attributes of IEEE 1815 and IEC 60870-5 Agent::60870andDNPNotification	65
Table 55 – Attributes of IEEE 1815 and IEC 60870-5 Agent::MasterAssociation	66
Table 56 – Attributes of IEEE 1815 and IEC 60870-5 Agent::OutstationAssociation	67
Table 57 – Attributes of ACSI::ACSISummary	70
Table 58 – Attributes of MMS::MMSProtocollInfo	72
Table 59 – Attributes of MMS::MMSProvider	73
Table 60 – Attributes of MMS::MMSAssociation	74

Table 61 – Attributes of MMS::MMSSecurityNotification	75
Table 62 – Attributes of MMS::MMSNotification	75
Table 63 – Attributes of SV and GSE common objects::GSEandSVCommon	76
Table 64 – Attributes of SV and GSE common objects::GSEandSVPublisherAssociation	77
Table 65 – Attributes of SV and GSE common objects::GSEandSVSubscriberAssociation	77
Table 66 – Attributes of SV::SVProvider	79
Table 67 – Attributes of SV::SVPublisherAssociationIP	79
Table 68 – Attributes of SV::SVPublisherAssociationL2	80
Table 69 – Attributes of SV::SVSubscriberAssociationIP	80
Table 70 – Attributes of SV::SVSubscriberAssociationL2	81
Table 71 – Attributes of SV::SVNotification	81
Table 72 – Attributes of GSE::GSESubscriberAssociation	83
Table 73 – Attributes of GSE::GSEProvider	83
Table 74 – Attributes of GSE::GSEPublisherAssociationIP	84
Table 75 – Attributes of GSE::GSEPublisherAssociationL2	84
Table 76 – Attributes of GSE::GSESubscriberAssociationIP	85
Table 77 – Attributes of GSE::GSESubscriberAssociationL2	85
Table 78 – Attributes of GSE::GSENotification	86
Table 79 – Attributes of Interfaces Agent::Interface	88
Table 80 – Attributes of Interfaces Agent::Interfaces	89
Table 81 – Attributes of Interfaces Agent::ETHEntry	90
Table 82 – Attributes of Interfaces Agent::KEYEntry	90
Table 83 – Attributes of Interfaces Agent::SEREntry	91
Table 84 – Attributes of Interfaces Agent::ALGEntry	91
Table 85 – Attributes of Interfaces Agent::USBEntry	92
Table 86 – Attributes of Interfaces Agent::Notification	92
Table 87 – Attributes of Clocks Agent::Clock	93
Table 88 – Attributes of Clocks Agent::ClockEntry	94
Table 89 – Attributes of Clocks Agent::SecurityNotification	95
Table B.1 – IEC 61850-7-4 objects mapping	229

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.

International Standard IEC 62351-7 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This edition of IEC 62351-7 cancels and replaces IEC TS 62351-7 Ed. 1 published in 2010. This new edition constitutes a technical revision and includes the following significant technical changes with respect to IEC TS 62351-7 (2010):

- a) NSM object data model reviewed and enriched;
- b) UML model adopted for NSM objects description;
- c) SNMP protocol MIBs translation included as Code Components.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
57/1857/FDIS	57/1885/RVD

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

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

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 IEC standard includes Code Components i.e components that are intended to be directly processed by a computer. Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labeled in this standard as a Code Component.

The purchase of this IEC standard carries a copyright license for the purchaser to sell software containing Code Components from this standard directly to end users and to end users via distributors, subject to IEC software licensing conditions, which can be found at: <http://www.iec.ch/CCv1>.

The Code Components included in this IEC standard are also available as electronic machine readable file at: http://www.iec.ch/tc57/supportdocuments/IEC_62351-7.MIBS.light.zip.

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

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

Part 7: Network and System Management (NSM) data object models

1 Scope

This part of IEC 62351 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 (Intelligent Electronic Devices), RTUs (Remote Terminal Units), DERs (Distributed Energy Resources) systems and other systems that are important to power system operations.

Power systems operations are increasingly reliant on information infrastructures, including communication networks, 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 telecontrol and automation protocols is already subject to health and condition monitoring control, using the concepts developed in the IETF Simple Network Management Protocol (SNMP) standards for network management. However, power system specific devices (like teleprotection, telecontrol, substation automation, synchrophasors, inverters and protections) need instead a specific solution for monitoring their health.

The NSM objects provide monitoring data for IEC protocols used for power systems (IEC 61850, IEC 60870-5-104) and device specific environmental and security status. As a derivative of IEC 60870-5-104, IEEE 1815 DNP3 is also 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 the sake of generality these data objects, and the data types of which they are comprised, are defined as abstract models of data objects.

In addition to the abstract model, in order to allow the integration of the monitoring of power system devices within the NSM environment in this part of IEC 62351, a mapping of objects to the SNMP protocol of Management Information Base (MIBs) is provided.

The objects that are already covered by existing MIBs are not defined here but are expected to be compliant with existing MIB standards.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

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

IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS¹*

IEC TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

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

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

IEEE 754:2008, *IEEE Standard for Floating-Point Arithmetic*

IETF RFC 2578, *Structure of Management Information Version 2 (SMIv2)*, April 1999, <http://tools.ietf.org/html/rfc2578>

IETF RFC 3410, *Introduction and Applicability Statements for Internet-Standard Management Framework*, December 2002, <http://tools.ietf.org/rfc/rfc3410>

IETF RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, December 2002, <http://tools.ietf.org/rfc/rfc3414>

IETF RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*, June 2004, <http://www.rfc-editor.org/rfc/rfc3826>

IETF RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*, March 2005, <http://tools.ietf.org/html/rfc4022>

IETF RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*, June 2005, <http://tools.ietf.org/html/rfc4113>

IETF RFC 4292, *IP Forwarding Table MIB*, April 2006, <http://www.rfc-editor.org/rfc/rfc4292>

IETF RFC 4293, *Management Information Base for the Internet Protocol (IP)*, April 2006, <http://tools.ietf.org/rfc/rfc4293>

IETF RFC 4898, *TCP Extended Statistics MIB*, May 2007, <http://tools.ietf.org/rfc/rfc4898>

IETF RFC 5132, *IP Multicast MIB*, December 2007, <http://tools.ietf.org/rfc/rfc5132>

IETF RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*, June 2010, <http://tools.ietf.org/rfc/rfc5905>

IETF RFC 5590, *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, June 2009, <http://tools.ietf.org/rfc/rfc5590>

¹ Under preparation. Stage at the time of publication: IEC CDV 62351-4:2017

IETF RFC 5591, *Transport Security Model for the Simple Network Management Protocol (SNMP)*, June 2009, <http://tools.ietf.org/rfc/rfc5591>

IETF RFC 5592, *Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)*, June 2009, <http://www.rfc-editor.org/rfc/rfc5592>

IETF RFC 5953, *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)*, August 2010, <http://www.rfc-editor.org/rfc/rfc5953>

IETF RFC 6347, *Datagram Transport Layer Security Version 1.2*, January 2012, <http://tools.ietf.org/rfc/rfc6347>

IETF RFC 6353, *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)*, July 2011, <http://tools.ietf.org/rfc/rfc6353>

IETF RFC 7860, *HMAC-SHA-2, Authentication Protocols in User-Based Security Model (USM) for SNMPv3*, April 2016, <http://tools.ietf.org/rfc/rfc7860>

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

Unified Modelling Language

UML

general-purpose modeling language with a semantic specification, a graphical notation, an interchange format, and a repository query interface, designed for use in object-oriented software applications, including those based on technologies recommended by the Object Management Group (OMG)

[SOURCE: ISO/IEC 19501:2005, Introduction]

3.2

Structure of Management Information

SMIv2

adapted subset of OSI's Abstract Syntax Notation One, ASN.1 used to write Management Information Base (MIB) modules (RFC 2578), which defines fundamental data types, an object model, and the rules for writing and revising MIB modules

[SOURCE: adapted from IETF RFC 3410, 7.1]

3.3

Transport Security Model

Security Model for the Simple Network Management Protocol for use with secure Transport Models in the Transport Subsystem

[SOURCE: adapted from IETF RFC 5590, 3.2.1]

3.4**Datagram Transport Layer Security**

protocol that provides communications privacy for datagram protocols, which allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery

Note 1 to entry: The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees.

[SOURCE: adapted from IETF RFC 6347, abstract]

3.5**Protocol Data Unit**

PDU

data object exchanged by protocol machines (entities) within a given layer, which consists of both Protocol Control Information (PCI) and user data

Note 1 to entry: This is OSI terminology for "packet".

[SOURCE: IETF RFC 1208, *A glossary of networking terms*]

3.6**Protocol Control Information**

protocol information added by an OSI entity to the service data unit passed down from the layer above, all together forming a Protocol Data Unit (PDU)

[SOURCE: IETF RFC 1208, *A glossary of networking terms*]

4 Abbreviated terms and acronyms

Additional abbreviated terms and acronyms are given in IEC 62351-2.

Term	Definition
ASN.1	Abstract Syntax Notation One
DER	Distributed Energy Resource
DTLS	Datagram Transport Layer Security
GIS	Geographical Information System
IED	Intelligent Electronic Device
MIB	Management Information Base
MMS	Manufacturing Message Specification
NSM	Network and System Management
PCI	Protocol Control Information
PDU	Protocol Data Unit
RTU	Remote Terminal Unit
SMI	Structure of Management Information
TLS	Transport Layer Security
TSM	Transport Security Model
UML	Unified Modelling Language

5 Overview of Network and System Management (NSM)

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 (Supervisory Control and Data Acquisition) 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 staff 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.

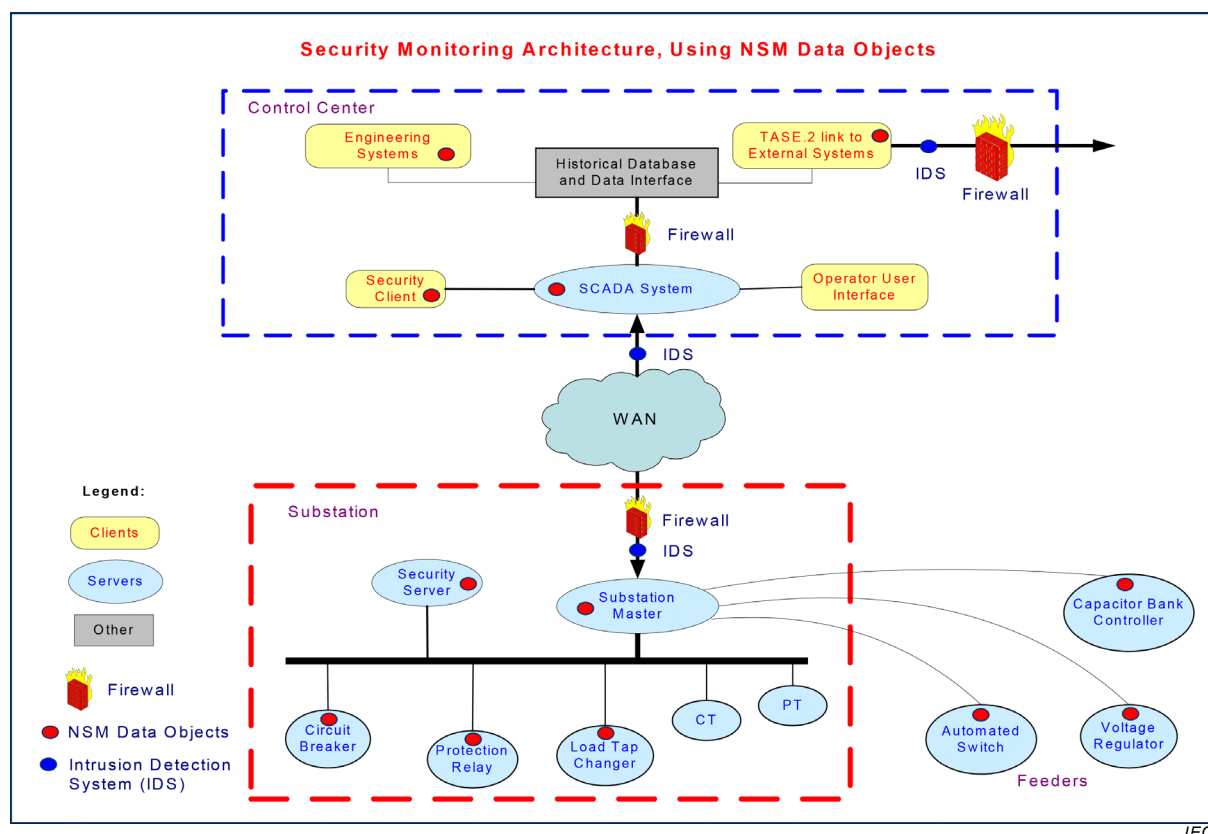


Figure 1 – Example of a power system SCADA architecture extended with NSM Data Objects

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 MIB is a database defining hierarchical data objects, with each object identified by 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 in a way to indicate the state of different equipment, applications, and systems.

Many systems use SNMP over internal communication networks as well. Due to 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 the ISO 7498-4 standard into five areas:

- Performance management;
- Configuration management;
- Accounting management;
- Fault management;
- Security management.

Of these five areas, only accounting management is not relevant to this standard. The other four 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 document 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 document 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 of this document.

5.2.4 Other NSM protocols

The NSM abstract objects defined in this document can be mapped in the future toward other protocols. This additional mapping may be defined as a specific standard addendum.

The IEC 61850 protocol can be an example of future mapping, but also Constrained Application Protocol (CoAP) can be considered for future mappings.

The basic requirement for a possible mapping is that the protocol must support the mapping of the abstract object semantics into the data object semantics of protocol itself. In addition, it is important that any mapping into another protocol should also be supported by appropriate Network Management tools and technologies.

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.

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 Role Based Access Control (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 the status of backup equipment, including the 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 IEDs involves a combination of internal and external assessments 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 IEDs 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;
- Valid control commands out of sequence as detected by the 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.

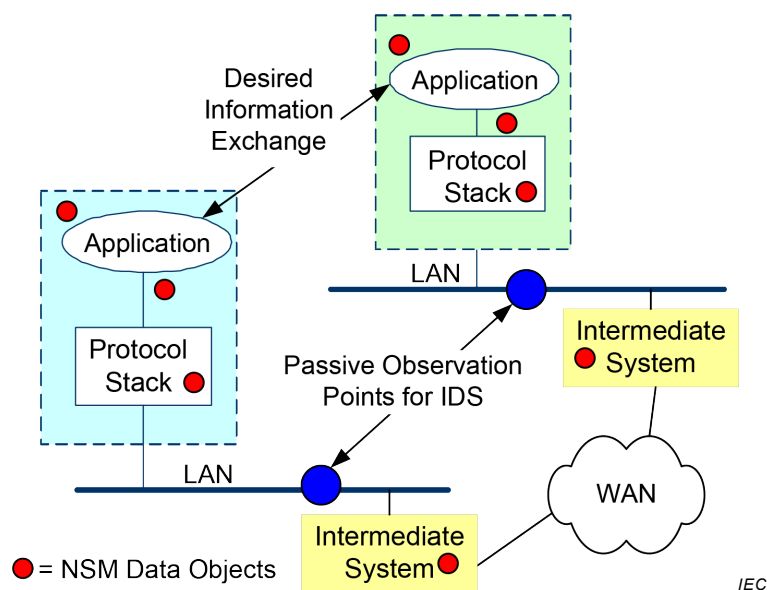


**Figure 2 – IDS Information exchange between applications:
generic communication topology**

Figure 2 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 sub clauses.

It must be noted that both IDS techniques rely on the communication availability toward a central management system, that shall be considered in the design of monitoring systems.

5.6.2 IDS: Passive observation techniques

Passive observation techniques (i.e. requiring no modifications to the system, communication 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.

Active security monitoring allows the collection of information that a passive probe could not be able to collect like high cpu usage, buffer overflow, certificate close to expire or invalid local access.

The collection of this information is in charge of a specific process running within the IED. This process collects internal measures and events and publishes the related values as related objects.

In this active security monitoring architecture, each layer in the protocol stack (depicted in Figure 3 with reference to ISO/OSI levels) would monitor for possible security attacks, and many applications would provide key error and failure data. A security provider would manage the NSM data objects, possibly setting appropriate thresholds, limits, and other parameters in order to fine-tune the response to more closely fit each power system operational environment. Upon the detection of an anomaly, the NSM data would be sent to the security manager for additional analysis. The target of these information are central Network Management Systems and all systems that need to collect the status and events. Operators have different responsibility and are not supposed to be the first endup.

This architecture is similar to the SNMP architecture. However, this does not imply that the SNMP formats will necessarily be used to transmit the NSM data: the NSM data objects would be implemented using whatever protocol is being used for other types of communications, as defined in 5.2.4.

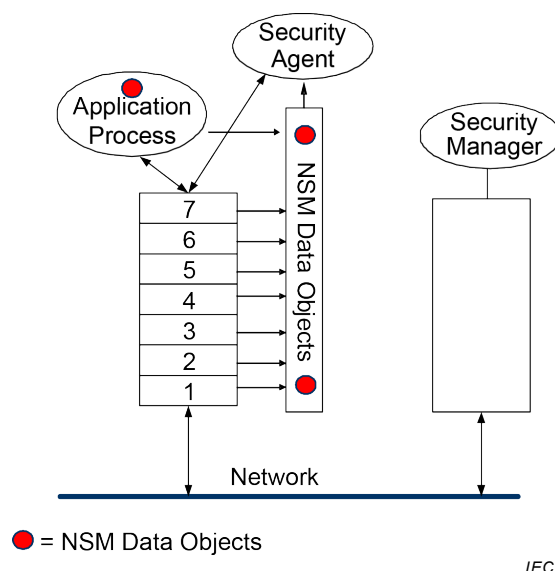


Figure 3 – Active security monitoring architecture with NSM data objects

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 three of the four security requirements: availability, 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 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 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 4, 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.

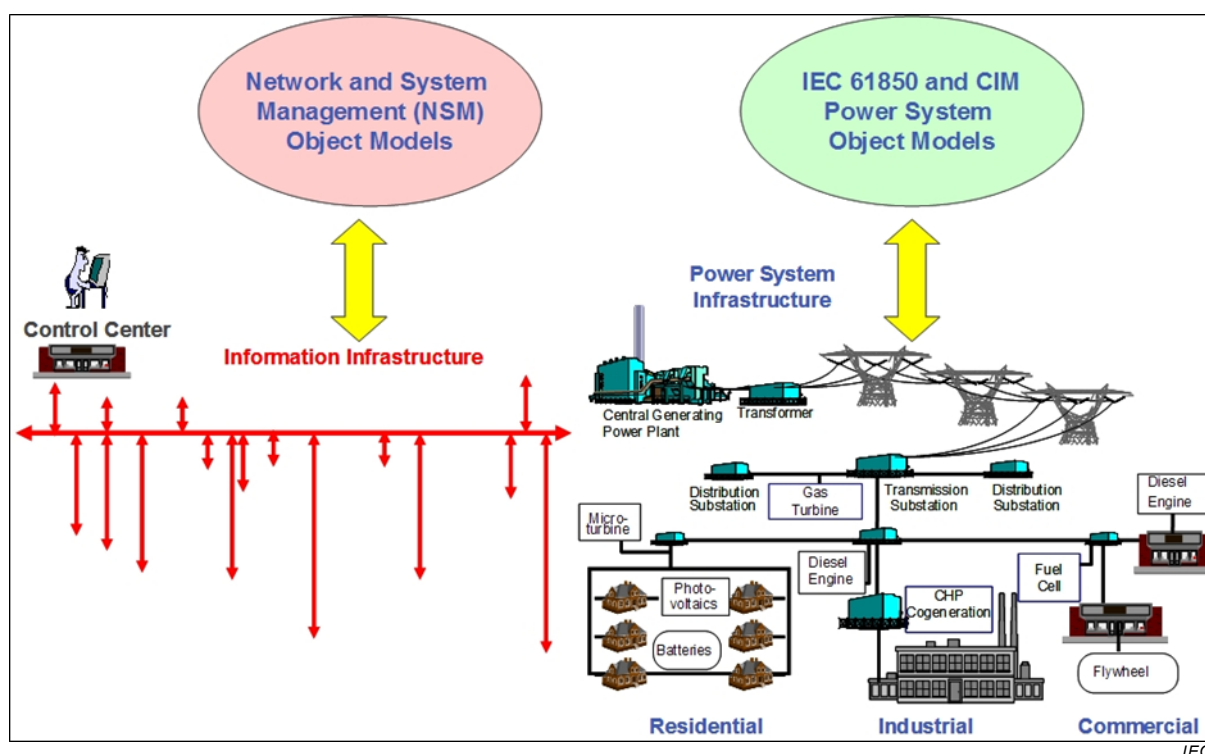


Figure 4 – Comparison of NSM data objects with IEC 61850 objects

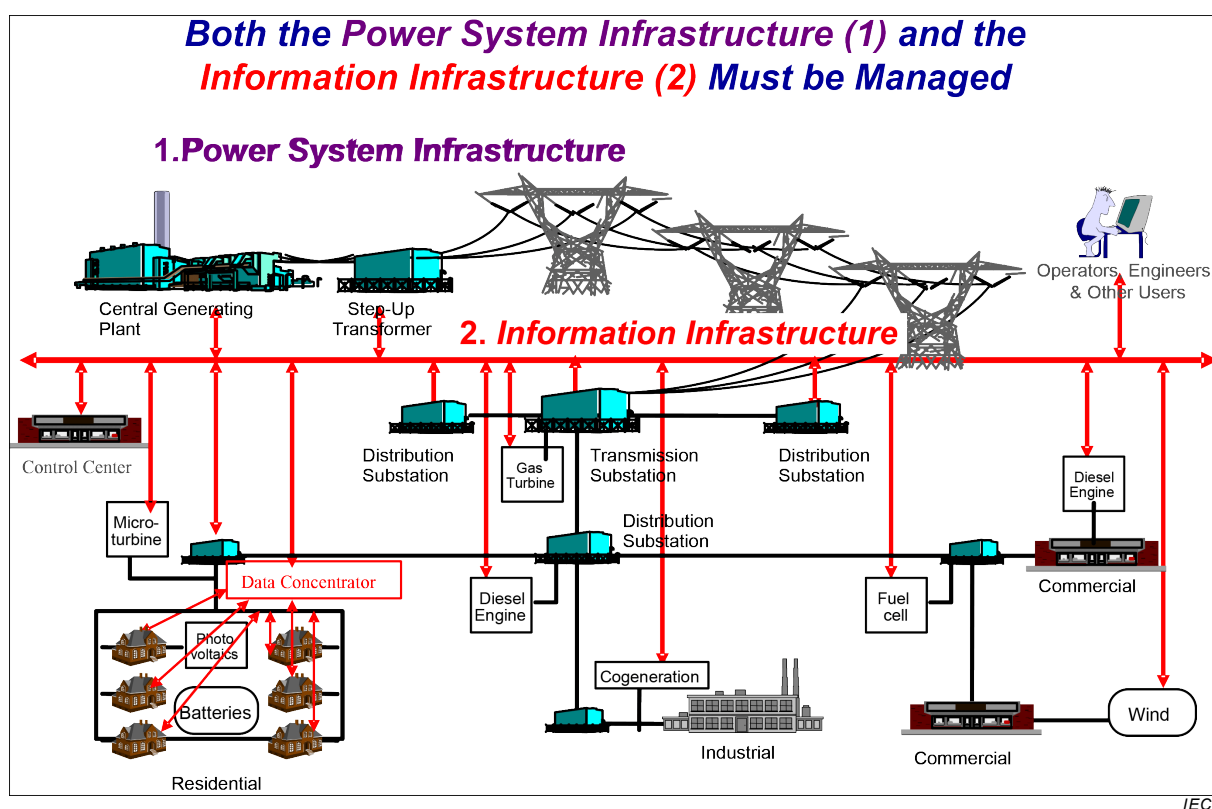


Figure 5 – Management of both the power system infrastructure and the information infrastructure

Not all of these security and reliability requirements can be filled by NSM, but many of them can be improved. Specifically, the following functions can be provided by NSM:

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

5.8 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 IEC 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 IEC 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 the 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 a SYN flood attack. The communication stack and applications do have an explicit knowledge of the resources, and this explicit knowledge of resources can be accessed through standardized NSM data objects.

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

- Exceeding the maximum number of connections permitted over the network;
- Count of number of connections actually in place over the network;
- Exceeding the maximum number of connections which can be in use simultaneously;
- Count of the number of connections in use simultaneously;
- Exceeding CPU load limits;

- Exceeding memory usage limits.

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

5.8.3 Detecting invalid buffer access DoS attacks

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

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

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

5.8.4 Detecting tampered/malformed PDUs

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

The NSM data objects in this category include:

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

5.8.5 Detecting physical access disruption

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

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

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

5.8.6 Detecting invalid network access

Firewalls are designed to prevent invalid access to networks, particularly through the use of access control lists which permit only authorized IP addresses to pass through the firewall. Other firewall capabilities include port restrictions, stateful filtering and session management.

However, internal (e.g. behind a firewall) resources can be converted into (inadvertent or deliberate) attackers. In many situations, this type of “conversion” is detectable by passive IDSs. However, IDSs within a network may not be able to recognize invalid data exchanges

which take place. For example, any protocols used both internally and externally, such as IEC 60870-6 (TASE.2) and IEC 61850-7-420 between control centres and other locations, 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, between control centres and to the dispersed facilities with DERs 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.

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 descriptions

5.9.1 Purpose of UML

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

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

UML supports the abstract description of objects and at the same time provides a complete collection of the information needed for the mapping to specific protocols. In other words the

semantics of abstract objects can be defined using UML description tools, where each object is described as a UML class or class attribute.

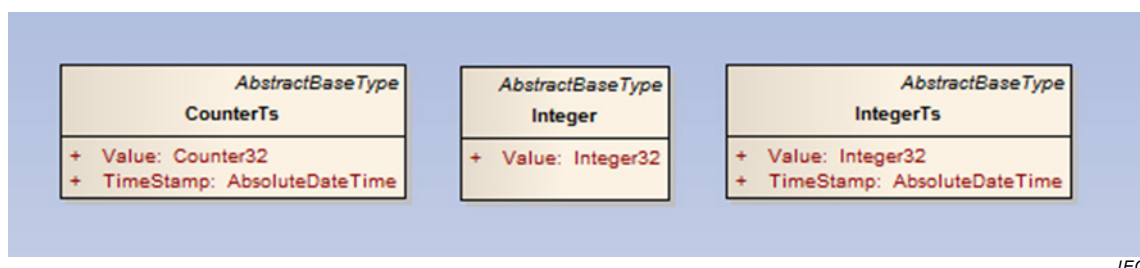
UML can be translated then into different real protocols notations (e.g. SNMP MIBs) through the adoption of an appropriate semantics translator that produces the specific protocol objects semantics according with the original UML description.

This standard introduces the IEC 62351-7 UML abstract objects model that includes:

- The description of the abstract types as a common list of objects (UML classes) that can be reused inside different monitoring agents.
- The description of the base types associated with SNMP mapping.
- The description of abstract classes providing attributes which are 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 to the agent or inherited from other 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 protocol objects. A further objective is the translation of those objects into SNMP MIB 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.



IEC

Figure 6 – Abstract types

Figure 6 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.

The BaseTypes package includes 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 package “EnumeratedTypes” provides the definition of enumerated values used for the abstract agent object attributes. Figure 7 depicts an example of the EnumeratedType declaration with the two types of “value only” and “value and timestamp” declaration.

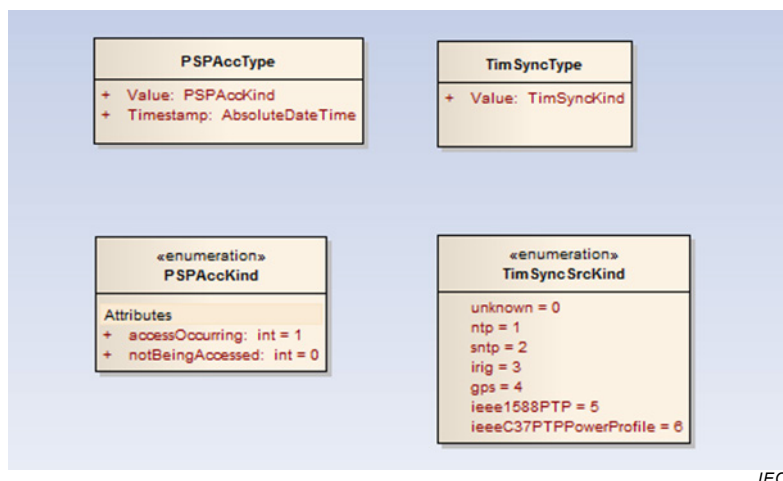


Figure 7 – Enumerated types

The concept of enumerated types declaration is almost the same as 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.

The concept of agent/subagent architecture (and the “agent/subagent” terminology) arises from the terminology of the SNMP NSM protocol. This standard uses this agent/subagent concept and the related architecture as an abstract idea.

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

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

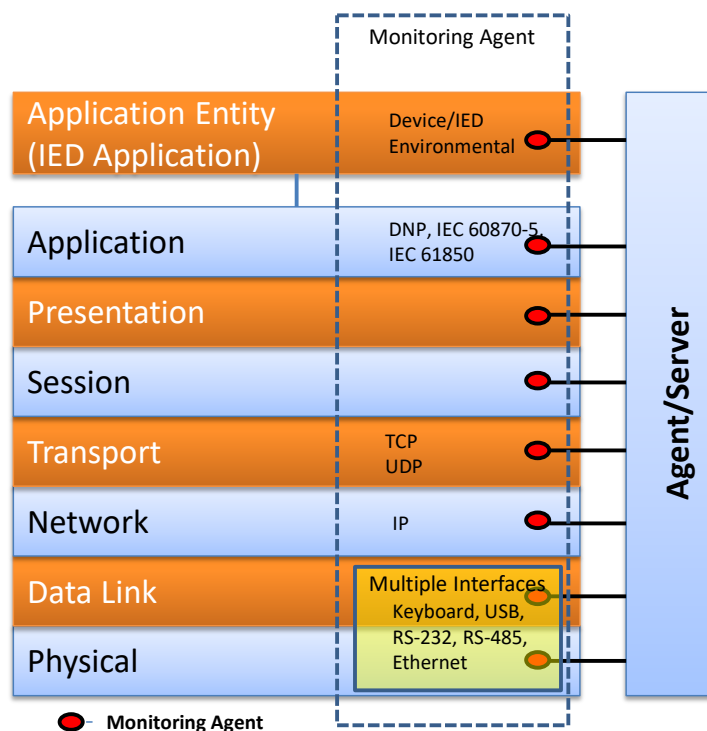
The homogenous set of objects include the following:

- Environmental Agent: device Physical and power security and health
- IED Agent: general device status (e.g. CPU, Storage, Certificate status)
- Application Protocol Agents: application protocols Statistics, status and alarms

- Interfaces Agent: The interfaces that need to be monitored are keyboards, USB, Serial, and Ethernet
- Clocks Agent: Status and health of clock synch system.

Each agent/subagent is responsible for updating values and related timestamps of its own instances of each abstract object.

Depending on the translation to a specific NSM protocol, the communication with the central NMS is delegated to one particular agent that acts as a communication mediator for the other agents which in this case act as subagents (this is the case of SNMP). Figure 8 provides a view of the agent/subagent hierarchy.



IEC

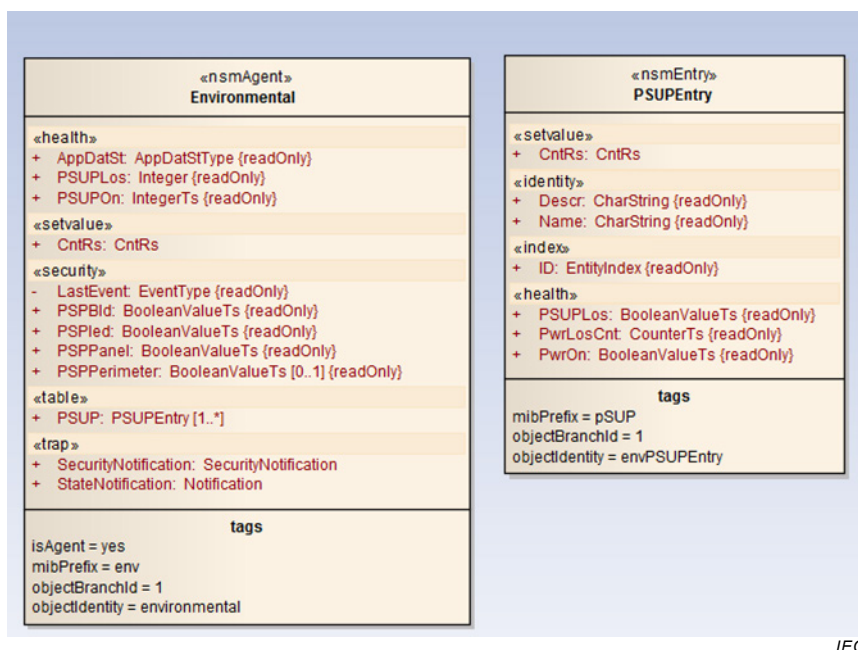
Figure 8 – Subagents

The agent/subagent structure is implemented using UML packages. Within each package the classes describe the following basic entities:

- UML classes having “nsmAgent” stereotype: these are the classes which contain as attributes the NSM abstract object
- UML classes having “nsmEntry” stereotype: these are the classes which contain subsidiary class.
- 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 commonly used by multiple agents. An agent can therefore inherit attributes from these common classes, avoiding attribute declaration duplication.

In Figure 9, the main Environmental agent is presented. 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.

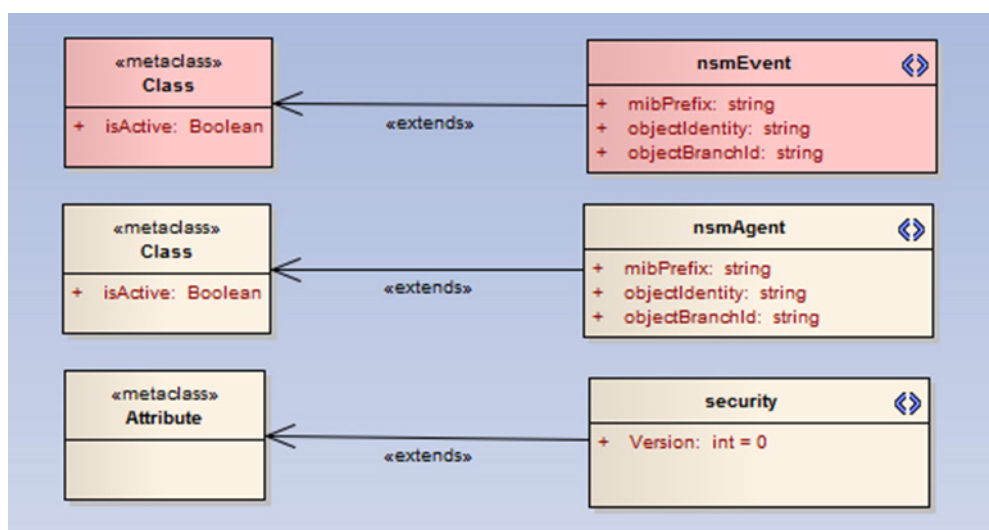


IEC

Figure 9 – Environmental agent

This kind of notation is always used in this UML model when a set of attributes must be supported in multiple instances (such as 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 which allows the declaration of a special class that includes the objects to be notified when a predefined event occurs.



IEC

Figure 10 – Model stereotypes

The nsmAgent stereotype declaration allows the use of an additional tool that includes some additional information for each class or attribute that is not strictly related to the abstract

model but is instead necessary for translating the model objects into SNMP MIBs (or also in the future to different protocols).

Therefore some stereotypes attributes are included and are 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.

5.9.6 UML Model extension

The UML model structure based upon the abstract agent concept allows several possible extension mechanisms of the structure and the related translations to specific protocols. Specifically, the following techniques can extend the current abstract object set:

- New abstract agent descriptions, for instance to define the abstract object related to a new protocol
- Additional classes included within existing abstract agents. For example these new classes can contain specific abstract objects for the monitoring of a new feature of an existing protocol
- New abstract objects can be added to existing abstract agent classes. The UML structure includes a version tagging mechanism to maintain the correct ordering of the new objects to come after existing objects.

Any new abstract agent or class can use UML inheritance to include any existing attributes.

5.10 Abstract Object UML translation to SNMP

5.10.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) was developed by the IETF as a protocol of level 7 OSI (IETF RFC 1157), 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 systems.

An agent is a software module that resides inside a managed device. This module is in charge of the exposure of NSM information via the 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 exposes that information in a form compatible with SNMP.

An SNMP agent can be present in a single managed device as multiple instances, for instance, being 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 allows an SNMP agent modular implementation with subagents also provided by independent manufacturer.

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

5.10.2 Management information bases (MIBs)

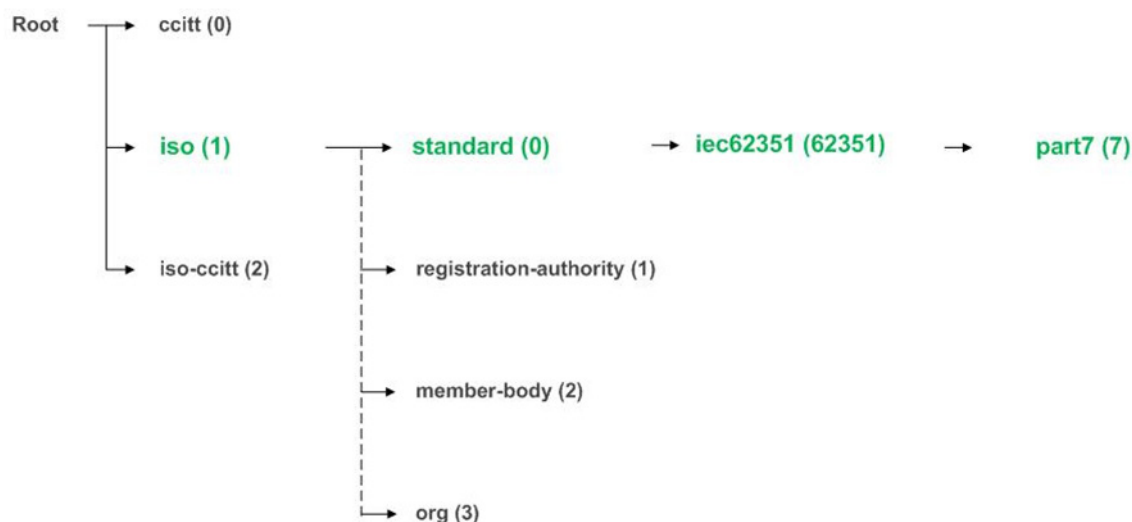
The variables accessible via SNMP are organized in hierarchies. The Management Information Bases (MIBs) are the entities that describe such hierarchies, together with the metadata such as type and description of the variable.

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), as shown in Figure 11. 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 (SMIv2, RFC 2578), that is a subset of ASN.1. Note that SMIv2 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 SMIv2 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.



IEC

Figure 11 – Object identifier structure

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 62351-7 is located under the iso branch. The full path is: iso.standard.iec62351.part7 (1.0.62351.7).

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

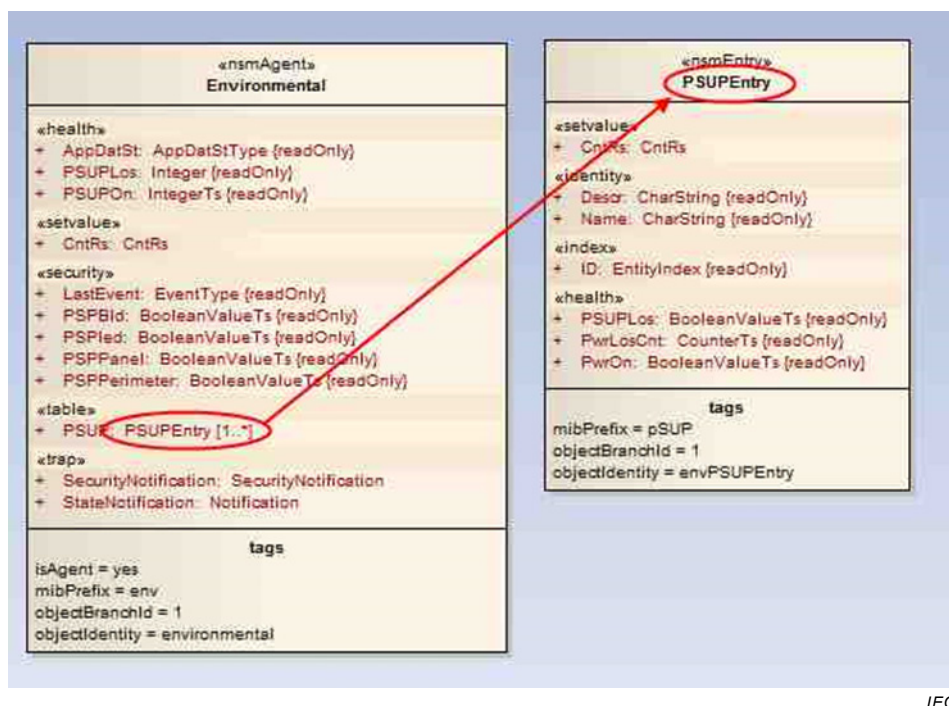
The translation of the objects defined in this standard and their semantics into SNMP object and semantics is carried out by adopting the following translation rules:

- The UML model package hierarchy starts 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:
 - 1) “objectIdentity” tag is the symbolic name of the branch.
 - 2) “objectBranchId” tag is the OID branch number.
- The EnumeratedTypes 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:
 - 1) “Value”: the actual abstract object value referring to the actual type, selected among the base types and used for SNMP object type assignment.
 - 2) “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.

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 constraint 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, thus declaring 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 existing list of SNMP MIB object of the same branch without affecting the SNMP OIDs mapping of existing MIB objects.

- The UML Model is translated into several SNMP MIBs. When a UML package include the “mibName” tag, the tag value is used as SNMP MIB name. Each MIB oid branch is produced according to the overall oid structure defined within the UML model.



IEC

Figure 12 – SNMP table

5.12 SNMP Security

SNMP Versions 1 and 2 do not implement a real authentication mechanism because they rely on a shared password (community string) that is sent in clear text between a manager and an agent.

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

SNMPv3 introduced the authentication feature that requires messages to include security parameters which are encoded as an octet string. SNMPv3 provides the following security features, as shown in Figure 13:

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

Figure 13 depicts the map of SNMP RFCs including SNMPv1, SNMPv2 and SNMPv3 protocol versions. The green marked RFCs are the relevant ones from the security perspective, while the yellow marked are related to SNMP transport and contain references to possible security countermeasures.

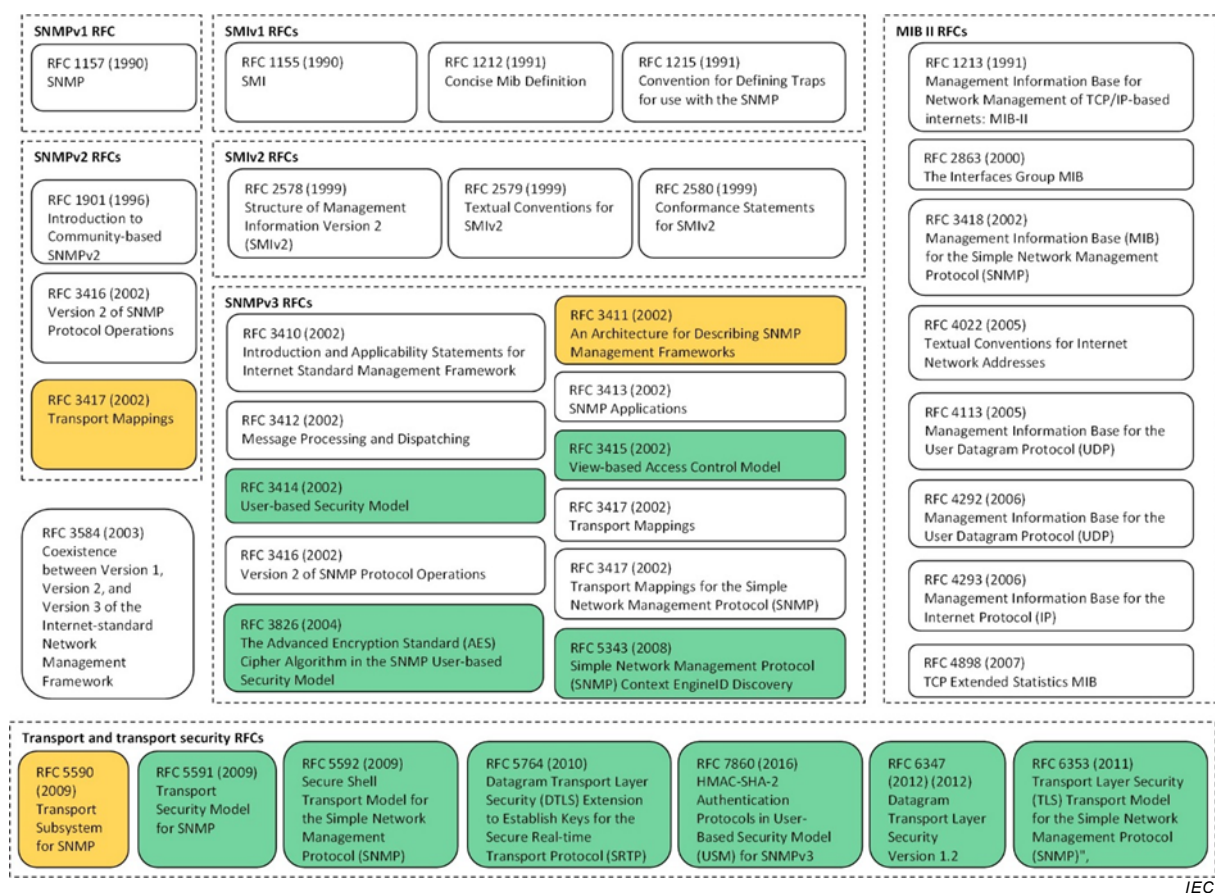


Figure 13 – SNMP RFCs map and security

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

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

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

RFC 3414 also includes a MIB document for remotely monitoring and managing the configuration parameters for the USM, the first and default SNMPv3 security model, including key distribution and key management. The User Security Model provides mechanisms for the following security features:

- Symmetric or private-key cryptography (username/passwords)
- Digest computation with keyed hashing algorithms (message integrity)
- Time indicators and automatic clock synchronization
- Data encryption

RFC 5590 includes the overall picture of SNMP transport, depicted in Figure 14. As shown in Figure 14, two end-to-end Security Models are available for SNMP: USM and Transport Security Model (TSM).

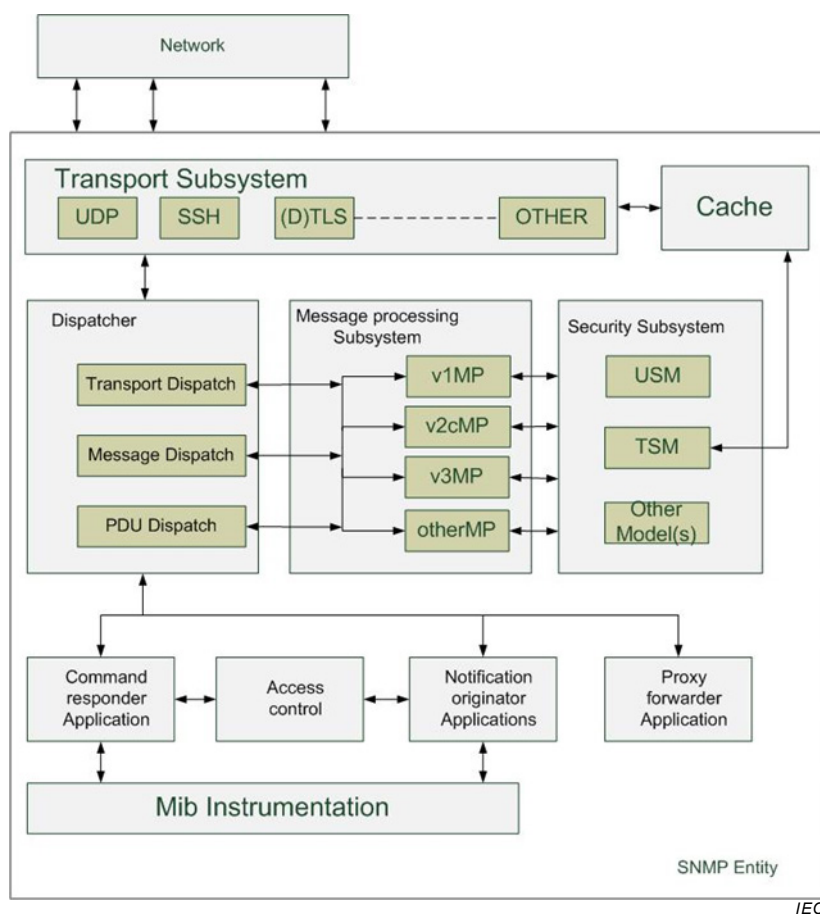


Figure 14 – SNMP Entity

RFC 5591, *Transport Security Model (TSM) for the Simple Network Management Protocol (SNMP)*, adds the TSM for SNMP. TSM defines a framework that allows the use of TLS and DTLS in order to provide a secure communication channel for SNMP messages.

Even if SNMP can be carried by several protocols, normally SNMP implementations are UDP based and therefore DTLS protocol support is included and actually suggested in TSM framework (RFC 5591, RFC 5592, RFC 5764, RFC 6347, RFC 6353).

According to RFC 5591 (chapter 8.1, “MIB Module Security”) SNMP versions prior to SNMPv3 did not include adequate security.

6 Abstract objects

6.1 General

This clause provides the higher level abstract object definitions that are reused inside the specific agents packages classes. In each diagram it should be noted that the arrow direction depicts the generalization of the class.

For implementations claiming conformance to this standard, the abstract objects defined in each agent section shall be implemented only when the related protocol or feature is provided by the device.

The mult column of the attributes table defines the multiplicity of each attribute. If the first number of multiplicity equals 0 then the attribute implementation is optional.

The authorization for resetting counters is a matter of Role Base Access Control that is defined in IEC TS 62351-8 and therefore is outside the scope of IEC 62351-7. The handling of authorization for resetting counters will be defined in specific future profiles of IEC 62351-7.

6.2 Package Abstract Types

6.2.1 General

The abstract objects used within each agent are mapped to the following object types, except for the objects that refer to special enumerated data types which are defined by their own dedicated types.

Abstract objects are classified by the following attributes:

- Type of data (Boolean, Counter, Integer, Float)
- Timestamp required for each status value change

The type object naming actually reflects this classification, as provided in the description of each abstract type.

It should be noted that the attribute defined in this package class exposes 1..1 multiplicity. The multiplicity is handled when these classes are used as attributes within the agents classes definition.

6.2.2 BooleanValue

BooleanValue is an abstract object reporting only a boolean variable.

Table 1 shows all attributes of BooleanValue.

Table 1 – Attributes of Abstract Types::BooleanValue

name	mult	type	Description
Value	1..1	TruthValue	Represents a boolean value.

6.2.3 BooleanValueTs

BooleanValueTs is an abstract object reporting a boolean value variable with a timestamp. The timestamp of the value change is stored into an auxiliary variable.

Table 2 shows all attributes of BooleanValueTs.

Table 2 – Attributes of Abstract Types::BooleanValueTs

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.
Value	1..1	TruthValue	Represents a boolean value.

6.2.4 CounterTs

CounterTs is an abstract object reporting an integer 32 value variable. A timestamp of value change is stored into an auxiliary variable.

Table 3 shows all attributes of CounterTs.

Table 3 – Attributes of Abstract Types::CounterTs

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.
Value	1..1	Counter32	According to SMI v2, used to specify a value which represents a count. The range is 0 to 4294967295.

6.2.5 CntRs

CntRs is an abstract object that allows a reset of the counters.

Table 4 shows all attributes of CntRs.

Table 4 – Attributes of Abstract Types::CntRs

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.
Value	1..1	TruthValue	Boolean

6.2.6 Floating

Floating is an abstract object reporting a Float32 value variable. IEEE Standard 754-2008 for Floating-Point Arithmetic.

Table 5 shows all attributes of Floating.

Table 5 – Attributes of Abstract Types::Floating

name	mult	type	description
Value	1..1	Float32TC	IEEE Standard 754-2008 for Floating-Point Arithmetic

6.2.7 FloatingTs

FloatingTs is an abstract object reporting a Float32 value variable and a timestamp. IEEE Standard 754-2008 for Floating-Point Arithmetic.

Table 6 shows all attributes of FloatingTs.

Table 6 – Attributes of Abstract Types::FloatingTs

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.
Value	1..1	Float32TC	IEEE Standard 754-2008 for Floating-Point Arithmetic

6.2.8 EntityIndex

EntityIndex is an abstract object reporting an unsigned Integer32 value variable used as Index entry to multiple instances of Class.

Table 7 shows all attributes of EntityIndex.

Table 7 – Attributes of Abstract Types::EntityIndex

name	mult	type	description
Value	1..1	Unsigned32	Integer value 1..2147483647 index

6.2.9 Integer

Integer is an abstract object reporting an Integer32 value variable.

Table 8 shows all attributes of Integer.

Table 8 – Attributes of Abstract Types::Integer

name	mult	type	description
Value	1..1	Integer32	Integer value 0 to Integer value - 2147483648..2147483647 (inclusive) according to SMI v2 according to SMI v2

6.2.10 IntegerTs

IntegerTs is an abstract object reporting an integer value variable and a timestamp. A timestamp of value change is stored into an auxiliary variable.

Table 9 shows all attributes of IntegerTs.

Table 9 – Attributes of Abstract Types::IntegerTs

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.
Value	1..1	Integer32	Integer value 0 to 4,294,967, 295 according to SMI v2

6.2.11 InetAddress

InetAddress denotes a generic Internet address. An InetAddress value is always interpreted within the context of an InetAddressType value. Every usage of the InetAddress textual convention is required to specify the InetAddressType object that provides the context. It is suggested that the InetAddressType object be logically registered before the object(s) that use the InetAddress textual convention, if they appear in the same logical row.

The value of an InetAddress object shall always be consistent with the value of the associated InetAddressType object. Attempts to set an InetAddress object to a value inconsistent with the associated InetAddressType shall fail with an inconsistent Value error.

Table 10 shows all attributes of InetAddress.

Table 10 – Attributes of Abstract Types::InetAddress

name	mult	type	description
Value	1..1	InetAddress	A value that represents an Internet address according to IETF RFC 4001.

6.2.12 InetAddressType

InetAddressType is an abstract object that represents a type of Internet address according to IETF RFC 4001.

Table 11 shows all attributes of InetAddressType.

Table 11 – Attributes of Abstract Types::InetAddressType

name	mult	type	description
Value	1..1	InetAddressType	Address Type

6.2.13 MacAddress

MacAddress is an abstract object that represents an 802 MAC address represented in the 'canonical' order defined by IEEE 802.1a, i.e., as if it were transmitted least significant bit first, even though 802.5 (in contrast to other 802.x protocols) requires MAC addresses to be transmitted most significant bit first.

Table 12 shows all attributes of MacAddress.

Table 12 – Attributes of Abstract Types::MacAddress

name	mult	type	description
Value	1..1	MacAddress	OCTET STRING (SIZE (6)), DISPLAY-HINT "1x:"

6.2.14 Selector

Selector is an abstract object used for T, S and P SELECTORS of a specific MMS association. It is a string formed using digits and letters from A to F. For Transport Selector, max length is 8. For Session and Presentation Selector, the max length is 16.

Table 13 shows all attributes of Selector.

Table 13 – Attributes of Abstract Types::Selector

name	mult	type	description
Value	1..1	DisplayString	For Transport Selector, max length is 8. For Session and Presentation Selector max length is 16.

6.2.15 Timestamp

Timestamp is an abstract object reporting a boolean value variable. A timestamp of the value change is stored in a related variable.

Table 14 shows all attributes of Timestamp.

Table 14 – Attributes of Abstract Types::Timestamp

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.

6.2.16 CharString

CharString is an abstract object reporting a String variable.

Table 15 shows all attributes of CharString.

Table 15 – Attributes of Abstract Types::CharString

name	mult	type	description
Value	1..1	DisplayString	Represents a String.

6.2.17 CharStringTs

CharStringTs is an abstract object reporting a String variable and a timestamp. A timestamp of value change is stored into an auxiliary variable.

Table 16 shows all attributes of CharStringTs.

Table 16 – Attributes of Abstract Types::CharStringTs

name	mult	type	description
TimeStamp	1..1	DateAndTime	Timestamp. The value of year is in network-byte order fractions of second is as defined in RFC 5905 epoch is defined as Midnight January 1, 1970.
Value	1..1	DisplayString	Represents a String.

6.2.18 AbstractBaseType root class

AbstractBaseType is the root UML class for abstract objects type UML classes.

6.2.19 AbstractAgent root class

AbstractAgent is the UML root class for agents UML classes.

6.3 Package EnumeratedTypes

6.3.1 General

The abstract objects defined as enumerated types refer to special enumerated data types.

The type object naming actually reflects this classification, as explained explicitly within this section in the description of each abstract type.

Please note that the attributes defined in this package classes have 1..1 multiplicity. The multiplicity is handled when these classes are used as attributes within the agents classes definition.

6.3.2 AppDatStKind enumeration

AppDatStKind is an enumeration of status for the environment where the device is operated (e.g. Power Supply, Physical Access).

Table 17 shows all literals of AppDatStKind.

Table 17 – Literals of EnumeratedTypes::AppDatStKind

literal	value	description
unknown	0	No information available about the environment.
good	1	Good environment status.
bad	2	Environmental problems detected.

6.3.3 PhyHealthKind enumeration

PhyHealthKind is an enumeration of general health status of IED.

Table 18 shows all literals of PhyHealthKind.

Table 18 – Literals of EnumeratedTypes::PhyHealthKind

literal	value	description
ok	0	No problems, normal operation.
warning	1	Minor problems, but in safe operation mode.
alarm	2	Severe problem, no operation possible.

6.3.4 ExtKind enumeration

ExtKind is an enumeration of possible IED extension types.

Table 19 shows all literals of ExtKind.

Table 19 – Literals of EnumeratedTypes::ExtKind

literal	value	description
unknown	0	unknown module
ioModule	1	I/O module
softwarePLC	2	Software PLC module

6.3.5 IntKind enumeration

IntKind is an enumeration of type of interface being utilized.

Table 20 shows all literals of IntKind.

Table 20 – Literals of EnumeratedTypes::IntKind

literal	value	description
wired	0	Wired interface
wireless	1	Wireless interface

6.3.6 LnkKind enumeration

LnkKind is an enumeration of LnkType.

Table 21 shows all literals of LnkKind.

Table 21 – Literals of EnumeratedTypes::LnkKind

literal	value	description
unknown	0	unknown
serial	1	serial
tcp	2	tcp
udp	3	udp
eth	4	Ethernet

6.3.7 PSPAccKind enumeration

PSPAccKind indicates that panel access is occurring at the IED.

Table 22 shows all literals of PSPAccKind.

Table 22 – Literals of EnumeratedTypes::PSPAccKind

literal	value	description
notBeingAccessed	0	No access to IED control panel is taking place.
accessOccurring	1	An access to IED control panel is taking place.

6.3.8 ProtIdKind enumeration

ProtIdKind is an enumeration used to identify the target protocol.