



IEC 62351-7

Edition 1.0 2017-07

INTERNATIONAL STANDARD



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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-4442-5

Warning! Make sure that you obtained this publication from an authorized distributor.

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	50

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	EXTEnter.....	56
7.3.5	STOREnter.....	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

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

Figure 3 – Active security monitoring architecture with NSM data objects

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

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	42

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 AC SI::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>