IEC 62351-7

Edition 1.0 2017-07

INTERNATIONAL STANDARD

colour inside

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

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 MMS*[1]

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