IEC

IEC TR 62351-90-3

Edition 1.0 2021-03

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 90-3: Guidelines for network and system management

IEC TR 62351-90-3:2021-03(en)

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TR 62351-90-3

Edition 1.0 2021-03

TECHNICAL REPORT

Power systems management and associated information exchange – Data and communications security – Part 90-3: Guidelines for network and system management

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-9529-8

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 90-3: Guidelines for network and system management

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.

IEC TR 62351-90-3 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is a Technical Report.

The text of this Technical Report is based on the following documents:

DTR	Report on voting
57/2255/DTR	57/2337/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under 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.

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 90-3: Guidelines for network and system management

1 Scope

This part of IEC 62351, which is a technical report, provides guidelines for efficiently handling both IT and OT data in terms of their monitoring, classification and correlations on them to deduce any possible useful outcomes about the state of the power system.

The convergence of information technologies (IT) and operational technologies (OT) refers to the integration of the systems, processes and data associated with the domains of IT and OT. This document provides guidelines for a comprehensive security monitoring for power grid components based on IT/OT convergent systems. The emphasis is about the development of a methodology and a set of recommendations for utility operators to build a general monitoring framework based on the analysis of the data collected from different IT and OT systems through network management, traffic inspection, and system activity readings. As such, the monitoring framework that this document introduces relies on the integration of management and logging information obtained using IEC 62351-7 and IEC 62351-14, respectively. Further systems and data sources from IT and OT would be considered such as the data obtained, for instance, through the IT network management using the Simple Network Management Protocol (SNMP), the passive network monitoring, and the functional characterization of control and automation processes.

This document's recommendations include the implementation of data collection, filtering and correlation mechanisms. The development of data analytics algorithms is out of the scope of this document and would be left to utility operators and owners. Finally, applications of the general monitoring framework guidelines and recommendations are provided for different power grid environments, namely for IEC 61850 substations and for Distributed Energy Resources (DER) systems.

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 and derivatives*

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 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

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

IEC TS 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber Security Event Logging*[1]

IEC TR 62351-90-2, *Power systems management and associated information exchange – Data and communications security – Part 90-2: Deep packet inspection of encrypted communications*

IEC TR 61850-90-4, *Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines*

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

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

IEEE 1815-2012, *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and IEC 62351-7 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

4 Abbreviated terms and acronyms

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

ASN.1	Abstract Syntax Notation One
DER	Distributed Energy Resource
DTLS	Datagram Transport Layer Security
DPI	Deep Packet Inspection
GIS	Geographical Information System
HMI	Human Machine Interface
ICS	Industrial Control System
IED	Intelligent Electronic Device

[1] Under preparation. Stage at the time of publication: IEC TS/PCC 62351-14:2021.

KDC	Key Distribution Center
MIB	Management Information Base
MMS	Manufacturing Message Specification
NSM	Network and System Management
NTS	Network Time Security
OID	Object IDentifier
PCI	Protocol Control Information
PLC	Programmable Logic Controller
PDU	Protocol Data Unit
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
TLS	Transport Layer Security
TSM	Transport Security Model
UML	Unified Modelling Language
USM	User-based Security Model

5 Information collection, filtering and processing

5.1 IT/OT elements

Converging IT/OT networks in a power grid include a wide range of components that allow the connection of systems together and communication in a local or wide area network. A brief overview of the elements is:

- IEDs, PLCs and RTUs – equipment connected with field sensors and actuators and able to coordinate with other elements through Ethernet and other means. These elements use protocols like IEC 60870-5-104/101 or IEEE 1815-2012 (protected with IEC 62351-3, IEC 62351-5), IEC 61850-8-1 and IEC 61850-8-2 (protected with IEC 62351-4), IEC 61850-8-1 and IEC 61850-9-2 (protected with IEC 62351-6), and other proprietary protocols for configuration and diagnostics.
- Substation controllers – are used within Substation Automation Systems to implement and automate controls, communication and monitoring. Also, these elements can use a variety of protocols like the ones mentioned above for IEDs, PLCs and RTUs.
- Gateways – implemented either as a software function or hardware, allow to connect elements in the network at application level, allowing a finer-grained segregation and/or a change of communication protocol.
- HMIs – equipment dedicated for human interaction, often purpose-built computers with touchscreens and software able to interact with the IEDs, PLCs and RTUs to understand the status of the system or change it using the protocols listed above.
- Computers and servers – more classical IT equipment with software able to interact with IEDs and similar devices. Many different kinds of protocols are used by these equipments, that can include standard protocols to interact with IEDs, PLCs and RTUs but also other standard and proprietary protocols to interact with other parts of the system.
- Switches, routers and firewalls – networking gear used to interconnect end systems together in an efficient and secure manner. These equipments support and can interact with a wide range of protocols like SSH, SNMP, Syslog, etc.

- VPN tunnels – generally composed of several sub-elements, can be implemented as software functions of other network elements like firewalls. They play an important role in IT/OT networks as they allow to interconnect different systems in a secure manner. From the other side, they are a critical part of the system as they may allow access to otherwise segregated networks.

Moreover, the way these components are provisioned and maintained is evolving. Virtualization for example has become a well-accepted tool also in OT systems to provide a reliable and flexible virtual version of most of the components above. Cloud computing on the other side is an established IT way to deploy services and systems and is becoming an emerging IT/OT integration technical mean that needs to be considered for the purposes of this document.

5.2 Network and system monitoring tools

5.2.1 SNMP monitoring agents

IEDs and also networking equipment implement SNMP mechanisms that are available today and will arrive/are arriving (IEC 62351-7) – SNMPv2c (most common) SNMPv1 (less common), SNMPv3 (more advanced and closer to IEC 62351-7).

It is interesting to note that network equipment come with both standard and vendor-specific MIBs that are well supported and accepted in the industry and provide a common set of information about generic health status of devices. In addition to these, the monitoring objects defined in IEC 62351-7 allow OT-specific information to be collected, thus allowing better control of the health and operational status of IEDs and similar devices.

The key takeaway is that SNMP is well-accepted and broadly implemented. It's important to remember that there are many MIBs, many versions and there is a need for some smart SNMP Manager able to support different versions and configurations (e.g. v2c, v3 with USM or TSM, etc) to normalize data and hide complexities (backward compatibility).

5.2.2 IDS/IPS probes

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are aimed at monitoring network communication packets and detecting any packet that is somehow foreign in a particular network. In such a case, the IDS will send an alert to a SIEM, leading the operators to execute appropriate actions following the intrusion detection and the identification of the vulnerability that is being exploited.

The substantial difference between IDS and IPS is that the first are aimed only to detect possible events informing other systems of the occurrence while IPS will also provide a possible direct reaction agains the detected threat (i.e. dropping a malicious connection). The choice between IDS and IPS should be dictated by either the need of a complete assurance of not affecting operation (IDS) or the desire to have some form of inline protection (IPS), at the cost of introducing delays due tue the fact that the packet need to pass its control logic and lack of complete control over network operation as detection techniques are subject to false positives.

Even if classical IDS/IPS systems are physical entities collecting traffic from switch/bridge/router mirror ports, the IDS/IPS function is often available in some other network devices (i.e. firewall or routers) or end systems as well.

The less disruptive passive observation techniques (i.e. requiring no modifications to the system, communication stack, or application) require only the addition of dedicated network-based IDS devices without any modification to the existing equipment, 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 in a much consolidated way.

IDS and IPS work using a "signature-based attack detection" approach through a pattern or behavioural recognition logic. This approach does not require accessing the semantics of traffic payload but IDS/IPS are able to detect the most of already known network attacks. These probes need of course a constant signature update process in order to keep the best possible detection capabilities. Anomaly-based approaches on the contrary permit to detect even unknown attacks after a learning phase, by highlighting baseline deviations – this approach allows the prevention of new attacks to be unnoticed but need further analysis by the user to understand how the deviation may affect the monitored systems. Modern IDS/IPS probes often combine both approaches.

To be effective in power grid systems, IDS probes need to be aware of the OT-specific devices, protocols and architectures in order to be able to detect the different kinds of threats. Another important effectiveness piece comes from the possibility to cope with encrypted communications and be able to identify issues encrypted traffic. In regards of IEC 62351-secured system (meaning the health of the end-to-end secure system), IEC TR 62351-90-2 contains an overview of how to apply DPI to IEC 62351-secured communications.

5.2.3 Network and system management central platforms

The NSM Operation center collects events and health status data from the devices through agents deployed inside the device itself and collecting information from IDS probes located in strategic positions on the telecommunication network.

Please note that the management data are collected from both ICS (OT systems) and corporate networks (IT systems). This approach is aimed at providing a stronger correlation between events arising from different perspectives.

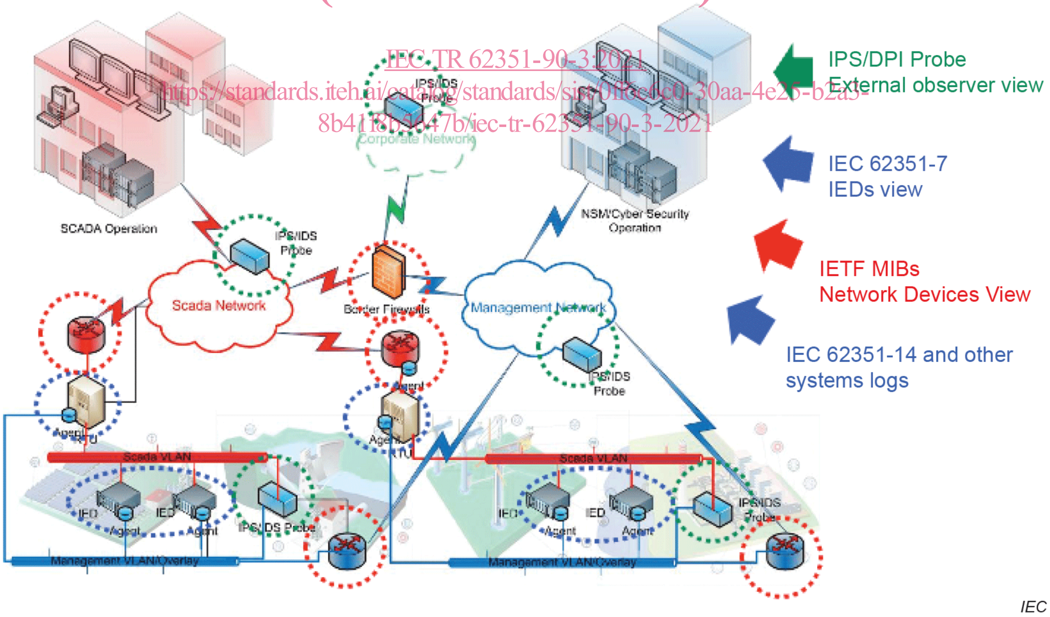

Figure 1 – NSM/Cybersecurity overall architecture

The left-hand side of Figure 1 depicts the OT operation perspective, in terms of SCADA systems and field devices, accessed with dedicated OT protocols.

The right-hand side depicts the Network and System Monitoring/Cyber Security operation center that is in charge of the collection of events and information from both IT and OT environments.