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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-9529-8

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

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 3
1 Scope 5
2 Normative references 5
3 Terms and definitions 6
4 Abbreviated terms and acronyms 6
5 Information collection, filtering and processing 7
5.1 IT/OT elements 7
5.2 Network and system monitoring tools 8
5.2.1 SNMP monitoring agents 8
5.2.2 IDS/IPS probes 8
5.2.3 Network and system management central platforms 9
5.3 Log management tools 10
5.3.1 Log collection architecture 10
5.3.2 Log agents 11
5.3.3 Log normalization 12
5.3.4 Security Information and Event Management (SIEM) 12
5.4 Other relevant data sources 12
6 Information correlation and presentation 13
6.1 Information selection and collection profiles 13
6.1.1 General 13
6.1.2 NSM and 62351-7 13
6.1.3 NSM and 61850-specific monitoring 16
6.1.4 NSM with other SNMP objects 16
6.1.5 Logs 17
6.2 Events, incidents and correlations 18
6.3 Security metrics (KPI) 18
6.4 Risk Management platforms 19
7 Monitoring use cases 19
7.1 General 19
7.2 Substation 19
7.3 DER systems 20
7.4 Large Hydro 20
7.5 Generation 20
8 Monitoring profiles for attack scenarios 20
8.1 General 20
8.2 Scenario: Malicious IED program change 20
8.3 Scenario: Unexpected 61850 Configuration 21
8.4 Scenario: Information gathering malware 21
Bibliography 22

Figure 1 – NSM/Cybersecurity overall architecture 9
Figure 2 – A logging infrastructure 11

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)*

---

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