IEC TR 62351-13

Edition 1.0 2016-08

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 13: Guidelines on security topics to be covered in standards and specifications

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-3571-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 13: Guidelines on security topics to be covered in standards and specifications

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 62351-13, which is a Technical Report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/1678/DTR	57/1727/RVC

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

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

A list of all parts in the IEC 62351 series, published 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 publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication 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.

INTRODUCTION

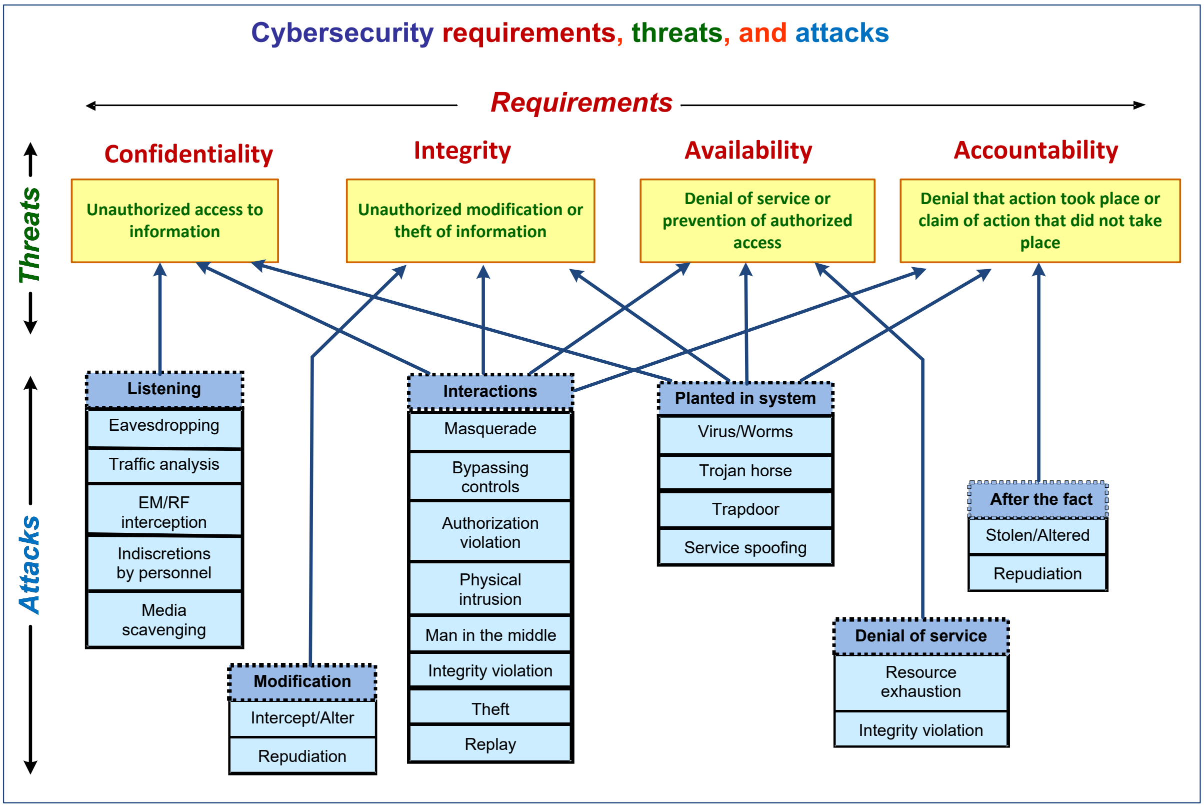
This document provides guidelines on what security topics should be covered in standards and specifications (IEC or otherwise) that are to be used in the power industry. These guidelines cannot be prescriptive for every standard, since individual standards and specifications may legitimately have very different focuses, but it should be expected that the combination of such standards and specifications used in any implementation should cover these security topics. These guidelines could therefore be used as a checklist for the combination of standards and specifications used in implementations of systems.

The security requirements for human users and software applications are different from the purely technical security requirements found in many communication and device standards. For user security standards, more emphasis should be on “policy and procedures” and “roles and authorization” rather than “bits and bytes” cryptographic technologies that should be included in Information and Communications Technology (ICT). In addition, engineering practices and system configurations should be taken into account, since no cryptography can compensate for poor design.

Figure 1 illustrates the relationships between security requirements, threats, and attacks.

This document is structured into four sections:

- Clause 5: Security requirements for standards and specifications which do not address specific cybersecurity technologies but where interactions between human users, software applications, and smart devices should be secured.
- Clause 6: Security requirements for standards and specifications that address information and communication technologies (ICT).
- Clause 7: Engineering design and configuration requirements that provide system reliability, defence in depth, and other security threat mitigations.
- Clause 8: Security requirements related to the OSI reference model.



IEC

Figure 1 – Security requirements, threats, and possible attacks

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

Part 13: Guidelines on security topics to be covered in standards and specifications

1 Scope

This part of IEC 62351, which is a Technical Report, provides guidelines on what security topics could or should be covered in standards and specifications (IEC or otherwise) that are to be used in the power industry, and the audience is therefore the developers of standards and specifications.

These guidelines cannot be prescriptive for every standard, since individual standards and specifications may legitimately have very different focuses, but it should be expected that the combination of such standards and specifications used in any implementation should cover these security topics. These guidelines are therefore to be used as a checklist for the combination of standards and specifications used in implementations of systems.

Out-of-scope are explicit methods for cyber security in product development, implementations, or operations.

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