IEC/TR 62351-10

Edition 1.0 2012-10

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 10: Security architecture guidelines

IEC/TR 62351-10:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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 corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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: csc@iec.ch.

IEC/TR 62351-10

Edition 1.0 2012-10

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 33.200

ISBN 978-2-83220-419-1

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 10: Security architecture guidelines

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 62351-10, 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
57/1234/DTR	57/1265/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 web site 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

Cyber security becomes more and more a basic necessity in power control systems as standard IT and other forms of modern communication technology are being increasingly used for control and supervision of these systems. The application of IT communication technology demands the consideration of already existing vulnerabilities, which can be exploited by potential attackers, as recent intentional and unintentional cyber incidents on SCADA and other industrial control systems have shown. The increasing number of control system cyber incidents world-wide with medium to high impact underlines the importance of appropriate security measures (see [11][1]).

The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 (Power Systems Management and Associated Information Exchange) is responsible for developing international standards for power system data communications protocols. Standards developed within TC 57 comprise for instance IEC 60870-5, IEC 61850, and IEC 62351 just to state a few. Especially the latter addresses technical security controls within power systems.

A security architecture as targeted here does not only comprise technical means like the application of dedicated security entities, security protocols or security options in communication protocols to secure power system entities or the communication network. It also describes operational guidelines considering the available technical base as well as the personnel controlling the power systems. Moreover, interactions with existing (security) infrastructures also affect overall system security.

In this Technical Report hands-on guidelines are proposed for the implementation of security mechanisms based on deployment examples, rather than a lecture or reference book for security in general. Therefore, available resources of information related to security of power systems or more general to security in Smart Grid are utilized and will be referenced as much as possible, without repeating their content here. Thus this Technical Report addresses both, the power system engineer and the traditional IT security engineer.

The examples used throughout this Technical Report are intended to better explain the influences of and the interactions with security. They are used as descriptive examples without the claim to be complete.

Clause 4 of this Technical Report specifies the specifics of the power systems industry, comprising differences in the security requirements compared to office systems as well as an overview about related standardization. It also introduces the TC 57 reference architecture as one base for the security architecture discussion.

Clause 5 establishes a general approach to a security architecture by using security domains and dedicated security controls within these domains and maps this approach to the power system domain based on examples use cases. Clause 5 also addresses the mapping of the NIST identified interface categories with the TC 57 architecture interfaces.

Clause 6 maps security controls with the IEC TC 57 power system architecture based on example scenarios. It starts with an overview scenario of power systems and digs into dedicated sub-scenarios like a substation deployment, the communication between a substation and a control centre and so on.

[1] References in square brackets refer to the Bibliography.

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

Part 10: Security architecture guidelines

1 Scope

This part of IEC 62351, which is a Technical Report, targets the description of security architecture guidelines for power systems based on essential security controls, i.e. on security-related components and functions and their interaction. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems is provided as a guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC/TS 62351-2, as well as the following apply.

3.1.1
de-militarized zone
DMZ
LAN segment / zone used to tier application/UI/file access between two other zones/segments

3.1.2
reliability
ability of a system to perform a required function under stated conditions for a specified period of time

3.1.3
security controls
technical or procedural security counter measures to avoid, counteract or minimize security risks

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ACL access control lists