IEC/TS 62351-2

Edition 1.0 2008-08

TECHNICAL SPECIFICATION

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

IEC/TS 62351-2:2008(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TS 62351-2

Edition 1.0 2008-08

TECHNICAL SPECIFICATION

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 2-8318-9956-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 2: Glossary of terms

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

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. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-2, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/853/DTS	57/922/RVC

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

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 publication will remain unchanged until the maintenance result 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

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual edition of this document may be issued at a later date.

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

Part 2: Glossary of terms

1 Scope and object

This part of IEC 62351 covers the key terms used in the IEC 62351 series, and is not meant to be a definitive list. Most terms used for cyber security are formally defined by other standards organizations, and so are included here with references to where they were originally defined.

2 Terms and definitions

2.1 Glossary references and permissions

With permission granted by the appropriate organizations, the definitions in this glossary were copied from the following sources:

- **[API 1164] American Petroleum Institute.** This standard on SCADA security provides guidance to the operators of Oil and Gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document is not limited to pipelines, but should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system. This document embodies the "API Security Guidelines for the Petroleum Industry." This guideline is specifically designed to provide the operators with a description of industry practices in SCADA Security, and to provide the framework needed to develop sound security practices within the operator's individual companies.

- **[ATIS]** ATIS Telecom Glossary 2007 at http://www.atis.org/glossary/. This web site incorporates and supersedes T1.523-2001, the ATIS Telecom Glossary of 2000 which was an expansion of FS-1037C, the Federal Standard 1037, *Glossary of Telecommunication Terms* initially published in 1980[1].

- **[FIPS-140-2]** This is the US Federal Information Processing Standard Publication 140-2, titled "*Security Requirements for Cryptographic Modules*".

- **[ISA99]** This ISA Technical Report provides a framework for developing an electronic security program and provides a recommended organization and structure for the security plan. The information provides detailed information about the minimum elements to include. Site or entity specific information should be included at the appropriate places in the program.

- **[ISO/IEC 27002:2005]** "Information technology - Security techniques - Code of practice for information security management" is an internationally-accepted standard of good practice for information security. This standard was originally the British Standard, BS7799, and later was termed ISO/IEC 17799, and was recently renamed to ISO/IEC 27002:2005.

[1] The ATIS Document Center is the leading, online resource to published and pre-published telecommunication standards, technical reports and requirements, guidelines produced by the ATIS sponsored industry forums and committees. The web site is http://www.atis.org Copyright © Alliance for Telecommunications Industry Solutions, 2001 in connection with all copyrightable subject matter created by and in Committee T1 and contained herein or comprised hereof. All Rights Reserved. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628-6380. ATIS is online at <http://www.atis.org>.

- **[ISO/IEC]** Many ISO/IEC documents contain term definitions that have been accepted as international standards. These documents are individually cited.
- **[NIST SP 800-53: December 2007]** National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems.
- **[NIST SP 800-82: September 2007]** National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems Security
- **[NIST SP 800-xx]** Other National Institute of Standards and Technology (NIST) documents are cited.
- **[NIST IR 7298]** National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms. This document usually cites other sources, which are therefore cited directly in this document.
- **[RFC 2828]** IETF RFC 2828 standard glossary of terms used for the Internet[2]

Other sources are cited as necessary.

[2] The Internet Society. Copyright I The Internet Society (2000). All Rights Reserved. This document (RFC 2828) and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

2.2 Glossary of security and related communication terms

2.2.1 Abstract Communication Service Interface (ACSI)

A virtual interface to an IED providing abstract communication services, e.g. connection, variable access, unsolicited data transfer, device control and file transfer services, independent of the actual communication stack and profiles used. [IEC 61850 series]

2.2.2 Access

The ability and means to communicate with or otherwise interact with a system in order to use system resources to either handle information or gain knowledge of the information the system contains. [RFC 2828]

2.2.3 Access Authority

An entity responsible for monitoring and granting access privileges for other authorized entities. [RFC 2828]

2.2.4 Access Control

1. Prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO/IEC 18028-2:2006]
2. Protection of resources against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. [RFC 2828]
3. Rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist. [ISO/IEC 27002:2005]

2.2.5 Access Control List (ACL)

A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources. [RFC 2828]

2.2.6 Accountability

1. The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO/IEC 7498-2]
2. The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions. [RFC 2828]

2.2.7 Adequate Security

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls. [NIST SP 800-53]