TECHNICAL SPECIFICATION

IEC TS 62351-1

First edition
2007-05

Power systems management and associated information exchange – Data and communications security

**Part 1:
Communication network and system security – Introduction to security issues**

Reference number
IEC/TS 62351-1:2007(E)

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

- 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 It also gives information on projects, withdrawn and replaced publications.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.

- 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

TECHNICAL SPECIFICATION

IEC TS 62351-1

First edition
2007-05

Power systems management and associated information exchange – Data and communications security

Part 1: Communication network and system security – Introduction to security issues

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 1: Communication network and system security – Introduction to security issues

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 62351-1, 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
57/802/DTS	57/850/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.

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

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 1: Communication network and system security – Introduction to security issues

1 Scope and object

1.1 Scope

The scope of the IEC 62351 series is information security for power system control operations. The primary objective is to "*Undertake the development of standards for security of the communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues*."

1.2 Object

Specific objectives include:

- IEC 62351-1 provides an introduction to the remaining parts of the standard, primarily to introduce the reader to various aspects of information security as applied to power system operations.
- IEC 62351-3 to IEC 62351-6 specify security standards for the IEC TC 57 communication protocols. These can be used to provide various levels of protocol security, depending upon the protocol and the parameters selected for a specific implementation. They have also been design for backward compatibility and phased implementations.
- IEC 62351-7 addresses one area among many possible areas of end-to-end information security, namely the enhancement of overall management of the communications networks supporting power system operations.
- Other parts are expected to follow to address more areas of information security.

The justification for developing these information security standards is that safety, security, and reliability have always been important issues in the design and operation of systems in the power industry, and information security is becoming increasingly important in this industry as it relies more and more on an information infrastructure. The deregulated market has imposed new threats as knowledge of assets of a competitor and the operation of his system can be beneficial and acquisition of such information is a possible reality. In addition, inadvertent actions (e.g. carelessness and natural disasters) can be as damaging as deliberate actions. Recently, the additional threat of terrorism has become more visible.

Although many definitions of "end-to-end" security exist, one (multi-statement) standard definition is "*1. Safeguarding information in a secure telecommunication system by cryptographic or protected distribution system means from point of origin to point of destination. 2. Safeguarding information in an information system from point of origin to point of destination*"[1]. Using this definition as a basis, the first four standards address the security enhancements for IEC TC 57 communication profiles, since these were identified as the obvious first steps in securing power system control operations. However, these security enhancements can only address the security requirements between two systems, but does not address true "end-to-end" security that covers internal security requirements, including

---

1 ATIS: an expansion of FS-1037C which is the US Federal Government standard glossary for telecommunications terms.

security policies, security enforcement, intrusion detection, internal system and application health, and all the broader security needs.

Therefore, the final sentence in the scope/purpose statement is very important: it is recognized that the addition of firewalls or just the simple use of encryption in protocols, for instance by adding "bump-in-the-wire" encryption boxes or even virtual private network (VPN) technologies would not be adequate for many situations. Security truly is an "end-to-end" requirement to ensure authenticated access to sensitive power system equipment, authorized access to sensitive market data, reliable and timely information on equipment functioning and failures, backup of critical systems, and audit capabilities that permit detection and reconstruction of crucial events.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of the IEC 62351 standard series.

IEC 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*

IEC 60870-6 (all parts), *Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations* [2]

IEC 61850 (all parts), *Communication networks and systems in substations*[3]

3 Terms, definitions and abbreviations

For the purposes of this part of IEC 62351, the terms and definitions given in IEC 62351-2 apply.

4 Background for information security standards

4.1 Rationale for addressing information security in power system operations

Communication protocols are one of the most critical parts of power system operations, responsible for retrieving information from field equipment and, vice versa, for sending control commands. Despite their key function, to date, these communication protocols have rarely incorporated any security measures, including security against inadvertent errors, power system equipment malfunctions, communications equipment failures, or deliberate sabotage. Since these protocols were very specialized, "Security by Obscurity" has been the primary approach. After all, only operators are allowed to control breakers from highly protected control centres. Who could possibly care about the megawatts on a line, or have the knowledge of how to read the idiosyncratic bits and bytes of the appropriate one-out-of-a-hundred communication protocols. And why would anyone want to disrupt power systems?

However, security by obscurity is no longer a valid concept. In particular, the electricity market is pressuring market participants to gain any edge they can. A tiny amount of information can turn a losing bid into a winning bid – or withholding that information from your competitor can make their winning bid into a losing bid. And the desire to disrupt power

[2] Also known as Inter-Control Centre Communications Protocol (ICCP) allows for data exchange over Wide Area Networks (WANs) between a utility control centre and other control centres, other utilities, power pools, regional control centres, and Non-Utility Generators.

[3] IEC 61850 which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control centre, and other power industry operational functions. It includes profiles to meet the ultra fast response times of protective relaying and for the sampling of measured values, as well as profiles focused on the monitoring and control of substation and field equipment.

system operations can stem from simple teenager bravado to competitive game-playing in the electrical marketplace to actual terrorism.

It is not only the market forces that are making security crucial. The sheer complexity of operating a power system has increased over the years, making equipment failures and operational mistakes more likely and their impact greater in scope and cost. In addition, the older, "obscure" communications protocols are being replaced by standardized, well-documented protocols that are more susceptible to hackers and industrial spies.

As the power industry relies increasingly on information to operate the power system, two infrastructures now have to be managed: not only the Power System Infrastructure, but also the Information Infrastructure. The management of the power system infrastructure has become reliant on the information infrastructure as automation continues to replace manual operations, as market forces demand more accurate and timely information, and as the power system equipment ages. Therefore, the reliability of the power system is increasingly affected by any problems that the information infrastructure might suffer.

4.2 IEC TC 57 data communications protocols

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. Its scope is "*To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control and Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations, and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems, and databases, which may be outside the scope of TC 57. The special conditions in a high voltage environment have to be taken into consideration.*"

IEC TC 57 has developed three widely accepted protocol standards, and has been the source of a fourth protocol. The three protocols are:

- **IEC 60870-5** which is widely used in Europe and other non-US countries for SCADA system to RTU data communications. It is used both in serial links (IEC 60870-5-101) and over networks (IEC 60870-5-104). **DNP3** was derived from IEC 60870-5 for use in the USA and now is widely used in many other countries as well, primarily for SCADA system to RTU data communications.
- **IEC 60870-6 (also known as TASE.2 or ICCP)** which is used internationally for communications between control centres and often for communications between SCADA systems and other engineering systems within control centres.
- **IEC 61850** which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control centre, and other power industry operational functions. It includes profiles to meet the ultra fast response times of protective relaying and for the sampling of measured values, as well as profiles focused on the monitoring and control of substation and field equipment.

These protocols are now widely used in the electric power industry. However, they were developed before information security became a major issue for the industry, so no security measures were included in the original standards.

4.3 History of the Development of these Security Standards

By 1997, IEC TC 57 recognized that security would be necessary for these protocols. It therefore first established a temporary group to study the issues of security. This group published a IEC/TR 62210 on the security requirements. One of the recommendations of

IEC/TR 62210 was to form a Working Group to develop security standards for the IEC TC 57 protocols and their derivatives.

The International Standards Organization (ISO) Common Criteria were originally selected as the method for determining the security requirements. This approach uses the concept of a Target of Evaluation (TOE) as the focus of a security analysis. However, determining what the characteristics of the TOE to protect became very cumbersome, given the multiplicity of different power system environments and the varying security needs, so ultimately it was not used. Threat-mitigation analysis (determining the most common threats and then developing security countermeasures for those threats) was used instead.

Therefore, IEC TC 57 WG 15 was formed in 1999, and has undertaken this work. The WG 15 title is "*Power system control and associated communications – Data and communication security*" and its scope and purpose are to "*Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues*."

The justification was that safety, security, and reliability have always been important issues in the design and operation of systems in the power industry, and cyber security is becoming increasingly important in this industry as it relies more and more on an information infrastructure. The deregulated market has imposed new threats as knowledge of assets of a competitor and the operation of his system can be beneficial and acquisition of such information is a possible reality. Recently, the additional threat of terrorism has become more visible.

The final sentence in the scope/purpose statement is very important: it was recognized that the addition of just simple encryption of the data, for instance by adding "bump-in-the-wire" encryption boxes or even virtual private network (VPN) technologies would not be adequate for many situations. Security truly is an "end-to-end" requirement to ensure authenticated access to sensitive power system equipment, reliable and timely information on equipment functioning and failures, backup of critical systems, and audit capabilities that permit reconstruction of crucial events.

5 Security issues for the IEC 62351 series

5.1 General information on security

This informative clause provides additional information on security issues that are not explicitly covered by these normative standards, but may be useful for understanding the context and scope of the normative standards.

5.2 Types of security threats

5.2.1 General

Security threats are generally viewed as the potential for attacks against assets. These assets can be physical equipment, computer hardware, buildings, and even people. However, in the cyber world, assets also include information, databases, and software applications. Therefore countermeasures to security threats should include protection against both physical attacks as well as cyber attacks.

Security threats to assets can result from inadvertent events as well as deliberate attacks. In fact, often more actual damage can result from safety breakdowns, equipment failures, carelessness, and natural disasters than from deliberate attacks. However, the reactions to successful deliberate attacks can have tremendous legal, social, and financial consequences that could far exceed the physical damage.

Utilities are accustomed to worrying about equipment failures and safety-related carelessness. Natural disasters are taken into consideration, particularly for utilities that commonly experience hurricanes, earthquakes, cyclones, ice storms, etc., even though these are looked upon as beyond the control of the utility. What is changing is the importance of protecting information which is becoming an increasingly important aspect of safe, reliable, and efficient power system operations.

Security risk assessment is vital in determining exactly what needs to be secured against what threats and to which degree of security. The key is determining the cost-benefit: "one size does not fit all"[4] (substations), layers of security are better than a single solution, and ultimately no protection against attacks can ever be completely absolute. Nonetheless, there is a significant space between the extremes from doing nothing to doing everything, to provide the level of security needed for modern utility operations.

The benefits also can flow the other way. If additional security is implemented against possible deliberate attacks, this monitoring can be used to improve safety, minimize carelessness, and improve the efficiency of equipment maintenance.

The following Subclauses discuss some of the most important threats to understand and to protect against. Most of these are covered by the IEC 62351 series, at least at the monitoring level.

5.2.2 Inadvertent threats

5.2.2.1 Safety failures

Safety has always been a primary concern for electric power utilities, particularly for those field crews working in the high voltage environments of substations. Meticulous procedures have been developed and refined over and over again to improve safety. Although these procedures are the most important component of a safety program, monitoring of the status of key equipment and the logging/alarming of compliance to the safety procedures through electronic means can enhance safety to a significant degree, and can benefit other purposes as well.

In particular, although access measures which permit only authorized personnel into substations have been implemented primarily for safety reasons, electronic monitoring of these safety measures can also help to prevent some deliberate attacks, such as vandalism and theft.

5.2.2.2 Equipment failures

Equipment failures are the most common and expected threats to the reliable operation of the power system. Significant work has been undertaken over the years to monitor the status of substation equipment, such as oil temperature, cooling systems, frequency deviations, voltage levels, and current overloads. This part of IEC 62351 does not focus on these types of monitoring except where the additional information can provide additional physical security.

However, often the monitoring of the physical status of equipment can also benefit maintenance efficiency, possible prevention of certain types of equipment failures, real-time detection of failures not previously monitored, and forensic analysis of equipment failure processes and impacts. Therefore, the total cost-benefit of some monitoring of physical security can be improved by taking these additional consequences into account.

---

[4] In the sense that one single solution cannot be used for all situations, so multiple solutions should be allowed.