# 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

PRICE CODE V

*For price, see current catalogue*

# CONTENTS

FOREWORD....4

1 Scope and object....6
1.1 Scope....6
1.2 Object....6
2 Normative references....7
3 Terms, definitions and abbreviations....7
4 Background for information security standards....7
4.1 Rationale for addressing information security in power system operations....7
4.2 IEC TC 57 data communications protocols....8
4.3 History of the Development of these Security Standards....8
5 Security issues for the IEC 62351 series....9
5.1 General information on security....9
5.2 Types of security threats....9
5.3 Security requirements, threats, vulnerabilities, attacks, and countermeasures....12
5.4 Importance of security policies....19
5.5 Security risk assessment....20
5.6 Understanding the security requirements and impact of security measures on power system operations....20
5.7 Five-step security process....21
5.8 Applying security to power system operations....23
6 Overview of the IEC 62351 series....24
6.1 Scope of the IEC 62351 series....24
6.2 Authentication as key security requirement....24
6.3 Objectives of the IEC 62351 series....24
6.4 Relationships between the IEC 62351 parts and IEC protocols....25
6.5 IEC 62351-1: Introduction....26
6.6 IEC 62351-2: Glossary of terms....26
6.7 IEC 62351-3: Profiles including TCP/IP....26
6.8 IEC 62351-4: Security for profiles that include MMS....28
6.9 IEC 62351-5: Security for IEC 60870-5 and derivatives....28
6.10 IEC 62351-6: Security for IEC 61850 Profiles....29
6.11 IEC 62351-7: Security through network and system management....31
7 Conclusions....34

Bibliography....35

Figure 1 – Security requirements, threats, and possible attacks....14
Figure 2 – Security categories, typical attacks, and common countermeasures....14
Figure 3 – Confidentiality security countermeasures....16
Figure 4 – Integrity security countermeasures....16
Figure 5 – Availability security countermeasures....17
Figure 6 – Non-repudiation security countermeasures....17
Figure 7 – Overall security: security requirements, threats, countermeasures, and management....18

Figure 8 – General security process – continuous cycle ..... 22
Figure 9 – Correlation between the IEC 62351 series and IEC TC 57 profile standards ..... 26
Figure 10 – Authentication security measure in GOOSE/SMV ..... 31
Figure 11 – NSM object models are the information infrastructure equivalent to the CIM and IEC 61850 object models of the power system infrastructure ..... 32
Figure 12 – Power system operations systems, illustrating the security monitoring architecture ..... 33

Table 1 – Characteristics of the three multicast IEC 61850 protocols ..... 30
Table 2 – Security measures for the three multicast IEC 61850 protocols ..... 30

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]

---

[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.