TECHNICAL REPORT

IEC TR 62210

First edition
2003-05

Power system control and associated communications – Data and communication security

Reference number
IEC/TR 62210:2003(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

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

TECHNICAL REPORT

IEC TR 62210

First edition
2003-05

Power system control and associated communications – Data and communication security

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE X

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEM CONTROL AND ASSOCIATED COMMUNICATIONS –

Data and communication security

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this technical report may be the subject of patent rights. The 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 62210, which is a technical report, has been prepared by IEC technical committee 57: Power system control and associated communications.

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

Enquiry draft	Report on voting
57/613/DTR	57/630/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.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

A bilingual version of this technical report may be issued at a later date.

POWER SYSTEM CONTROL AND ASSOCIATED COMMUNICATIONS –

Data and communication security

1 Scope and object

This Technical Report applies to computerised supervision, control, metering, and protection systems in electrical utilities. It deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems.

NOTE This report does not include recommendations or criteria development associated with physical security issues.

Realistic threats to the system and its operation are discussed. The vulnerability and the consequences of intrusion are exemplified. Actions and countermeasures to improve the current situation are discussed but solutions are to be considered issues for future work items.

2 Overview

Safety, security, and reliability have always been important issues in the design and operation of systems in electrical utilities. Supervision, protection, and control system have been designed with the highest possible level of safety, security, and reliability. The communication protocols have been developed with a residual error rate approaching zero. All these measures have been taken to minimise the risk of danger for personnel and equipment and to promote an efficient operation of the power network.

Physical threats on vulnerable objects have been handled in the classical ways by locked buildings, fences and guards but the quite possible terrorist threat of tripping a critical breaker by a faked SCADA command on a tapped communication link has been neglected. There is no function in the currently used protocols that ensure that the control command comes from an authorised source.

The deregulated electricity market has imposed new threats: knowledge of the assets of a competitor and the operation of his system can be beneficial and acquisition of such information is a possible reality.

The communication protocols and systems need protection from advertent and inadvertent intruders, the more the protocols are open and standardised and the more the communication system is integrated in the corporate and world-wide communication network.

This Technical Report discusses the security process of the electrical utility. The security process involves the corporate security policy, the communication network security, and the (end-to-end) application security.

The security of the total system depends on secure network devices, i.e. the security of any device that can communicate. A secure network device has to be capable of performing ‘safe’ communication and of authenticating the access level of the user. Intrusive attacks have to be efficiently detected, recorded and prosecuted as part of an active audit system.

The threats are analysed based on possible consequences to a system, i.e. what is the worst that could happen if an illicit intruder has ambition and resources? The vulnerability of a utility and its assets are analysed together with the threats.

Having shown that there exists threats to vulnerable points in the systems of electrical utilities the countermeasures are discussed with special focus on the communication protocols defined by IEC Technical Committee 57: the IEC 60870-5 series, the IEC 61334 series, the IEC 60870-6 series and the IEC 61850 series.

Proposals on new work items to include security aspects in these protocols are given.

3 Reference documents

The following referenced documents are indispensable for the application 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 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*

IEC 61334 (all parts), *Distribution automation using distribution line carrier systems*

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

ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*

ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*

ISO/IEC 10181-7:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 2: Security functional requirements*

ISO/IEC 15408-3, *Information technology – Security techniques – Evaluation criteria for IT Security – Part 3: Security assurance requirements*

4 Terms, definitions and abbreviations

4.1 Terms and definitions

4.1.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

4.1.2
asset
Anything that has value to the organisation

[ISO/IEC TR 13335-1:1997]

4.1.3
authenticity
property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information

4.1.4
authorisation violation
entity authorised to use a system for one purpose uses it for another, unauthorised purpose

4.1.5
availability
property of being accessible and usable upon demand by an authorised entity

[ISO 7498-2: 1989]

4.1.6
baseline controls
minimum set of safeguards established for a system or organisation

[ISO/IEC TR 13335-1:1997]

4.1.7
confidentiality
property that information is not made available or disclosed to unauthorised individuals, entities, or processes

[ISO 7498-2:1989]

4.1.8
data integrity
property that data has not been altered or destroyed in an unauthorised manner

[ISO 7498-2:1989]

4.1.9
denial of service
authorised communications flow is intentionally impeded

4.1.10
eavesdropping
information is revealed to an unauthorised person monitoring communication traffic

4.1.11
hack
threat that may be a combination of one or more of the following threats: authorisation violation; information leakage; integrity violation; and masquerade

4.1.12
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values

4.1.13
information leakage
unauthorised entity obtains secure/restricted information

4.1.14
integrity violation
information is created or modified by an unauthorised entity

4.1.15
intercept/alter
communication packet is intercepted, modified, and then forwarded as if it were the original packet

4.1.16
masquerade
unauthorised entity attempts to assume the identity of a trusted party

4.1.17
reliability
property of consistent intended behaviour and results

[ISO/IEC TR 13335-1:1997]

4.1.18
replay
communication packet is recorded and then retransmitted at an inopportune time

4.1.19
repudiation
exchange of information occurs and one of the two entities in the exchange later denies the exchange or contents of the exchange

4.1.20
residual risk
risk that remains after safeguards have been implemented

[ISO/IEC TR 13335-1:1997]

4.1.21
resource exhaustion
see denial of service

4.1.22
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

[ISO/IEC TR 13335-1:1997]

4.1.23
security auditor
individual or a process allowed to have access to the security audit trail and to build audit reports

[ISO/IEC 10181-7:1996]

4.1.24
security authority
entity that is responsible for the definition, implementation or enforcement of security policy

4.1.25
security domain
set of elements, a security policy, a security authority, and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

4.1.26
security domain authority
security authority that is responsible for the implementation of a security policy for a security domain

4.1.27
security token
set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities

4.1.28
security-related event
any event that has been defined by security policy to be a potential breach of security, or to have possible security relevance. Reaching a pre-defined threshold value is an example of a security-related event

4.1.29
spoof
combination of one or more of the following threats: eavesdropping; information leakage; integrity violation; intercept/alter; and masquerade

4.1.30
system integrity
property that a system performs its intended functions in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system

[ISO/IEC TR 13335-1:1997]

4.1.31
threat
potential cause of an unwanted incident which may result in harm to a system or organisation

[ISO/IEC TR 13335-1:1997]

4.1.32
trust
entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities

4.1.33
trusted entity
entity which is assumed to appropriately enforce security policies. Because of this assumption, the entity may cause other security policies to be obviated.

EXAMPLE A trusted authorisation entity declares a user to be authorised for control thereby challenges authentication procedures, that would normally be applied, are not invoked.

Entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do

4.1.34
vulnerability
includes a weakness of an asset, or group of assets, which can be explained by a threat

[ISO/IEC TR 13335-1:1997]

4.1.35
developed technology
software code/algorithms that are developed within the configuration and guidelines for quality and security assurance set forth as EAL-5, or greater, as specified in ISO/IEC 15408-3

4.2 Abbreviations

AMR	Automatic Meter Reading
CC	Common Criteria
COTS	Commercial off the shelf software
DISCO	Distribution Company
DLC	Distribution Line Carrier
DLMS	Distribution Line Messaging System
DMS	Distribution Management System
EAL	Evaluation Assurance Level
EMS	Energy Management System
GENCO	Generation Company
HMI	Human – Machine Interface (for example: operator workstation)
HV	High Voltage
IED	Intelligent Electronic Device
IT	Information Technology
LAN	Local Area Network
LV	Low Voltage
MMS	Manufacturing Message Specification
MV	Medium Voltage
NT	Windows NT is a Microsoft Windows personal computer operating system designed for users and businesses needing advanced capabilities
OASIS	Open Access Same-Time Information System
PLC	(user) Programmable Logic Controller
POTS	Plain Old Telephone System
PP	Protection Profile
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
ST	Security Target
TASE	Telecontrol Application Service Element
TCP/IP	Transmission Control Protocol/ Internetworking Protocol
TOE	Target of Evaluation
TRANSCO	Transmission Company
VAA	Virtual Application Association
VDE	Virtual Distribution Equipment
WAN	Wide Area Network