TECHNICAL REPORT

IEC TR 62210

First edition
2003-05

Power system control and associated communications – Data and communication security

© IEC 2003 — Copyright - all rights reserved

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

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

FOREWORD 4

1 Scope and object 5
2 Overview 5
3 Reference documents 6
4 Terms, definitions and abbreviations 6
4.1 Terms and definitions 6
4.2 Abbreviations 10
5 Introduction to security 11
5.1 How to use this report 11
6 The security analysis process 12
6.1 Network topologies 14
6.2 User consequence based analysis 16
6.2.1 Stakeholders 16
6.3 Consequences to be considered 18
6.3.1 Financial 18
6.3.2 Asset destruction/degradation 19
6.3.3 Inability to restore service 20
6.4 Consequences and security threats 20
7 Focus of security work within this report 22
7.1 Justification of application level security focus 22
7.2 Security analysis technique 23
7.2.1 Security objectives 23
7.2.2 General threats 24
7.2.3 Specific threats to be considered in PP 24
8 Vulnerabilities 27
8.1 Threats to topologies 27
8.2 Current IEC Technical Committee 57 protocols 29
8.2.1 TASE.1 29
8.2.2 TASE.2 30
8.2.3 IEC 60870-5 30
8.2.4 IEC 61334 30
8.2.5 IEC 61850 31
9 Recommendations for future IEC Technical Committee 57 security work 32

Annex A (informative) What is a protection profile? 35
Annex B (informative) Protection profile for TASE.2 37
Annex C (Informative) Example of consequence diagrams 43

Figure 1 – Normal corporate security process 12
Figure 2 – Business information flow 14
Figure 3 – General communication topology 16
Figure 4 – Consequence diagram: inability to restore service 21

Figure 5 – WAN/LAN topology....27
Figure 6 – Levels of vulnerability....28

Table 1 – Matrix to determine business process importance....17
Table 2 – Asset to business process relationships....20
Table 3 – Communication model security matrix....22

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*