IEC/PAS 62443-3

Edition 1.0 2008-01

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

Security for industrial process measurement and control – Network and system security

IEC/PAS 62443-3:2008(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 It also gives information on projects, withdrawn and replaced publications.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.

- 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/PAS 62443-3

Edition 1.0 2008-01

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

Security for industrial process measurement and control – Network and system security

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XA

ICS 25.040.40; 35.110

ISBN 2-8318-9543-X

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL – NETWORK AND SYSTEM SECURITY

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.

A PAS is a technical specification not fulfilling the requirements for a standard but made available to the public.

IEC-PAS 62443-3 has been processed by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
65/402/NP	65/412/RVN

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned will transform it into an International Standard.

This publication seeks the status of a basic security publication according to IEC Guide 104.

This PAS shall remain valid for an initial maximum period of three years starting from 2008-01. The validity may be extended for a single three-year period, following which it shall be revised to become another type of normative document or shall be withdrawn.

INTRODUCTION

The increasing degree of public networking of formerly isolated automation systems increases the exposure of such systems to attack. Standard IT security protection mechanisms have protection goals and strategies that may be inappropriate for automation systems. This PAS addresses the topic of securing access to and within industrial systems while assuring timely response which may be critical to plant operation.

For safety applications and applications in the pharmaceutical or other highly specialized industries, additional standards, guidelines, definitions and stipulations may apply, for example, IEC 61508, GAMP (ISPE), for GMP Compliance 21 CFR (FDA) and the Standard Operating Procedure of the European Medicines Agency (SOP/INSP/2003).

SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL – NETWORK AND SYSTEM SECURITY

1 Scope

This PAS establishes a framework for securing information and communication technology aspects of industrial process measurement and control systems including its networks and devices on those networks, during the operational phase of the plant's life cycle.

This PAS provides guidance on a plant's operational security requirements and is primarily intended for automation system owners/operators (responsible for ICS operation)

Furthermore, the operational requirements of this PAS may interest ICS stakeholders such as:

a) automation system designers;

b) manufacturers (vendors) of devices, subsystems, and systems;

c) integrators of subsystems and systems.

The PAS allows for the following concerns:

- graceful migration/evolution of existing systems;
- meeting security objectives with existing COTS technologies and products;
- assurance of reliability/availability of the secured communications services;
- applicability to systems of any size and risk (scalability);
- coexistence of safety, legal and regulatory and automation functionality requirements with security requirements.

NOTE 1 Plants and systems may contain safety critical components and devices. Any safety-related security components may be subject to certification based on IEC 61508 and according to the SILs therein. This PAS does not guarantee that its specifications are all or in part appropriate or sufficient for the security of such safety critical components and devices.

NOTE 2 This PAS does not include requirements for security assurance evaluation and testing.

NOTE 3 The measures provided by this PAS are rather process-based and general in nature than technically specific or prescriptive in terms of technical countermeasures and configurations.

NOTE 4 The procedures of this PAS are written with the plant owner/operator's mind set.

NOTE 5 This PAS does not cover the concept, design and implementation live cycle processes, i.e. requirements on control equipment manufacturer's future product development cycle.

NOTE 6 This PAS does not cover the integration of components and subsystems into a system.

NOTE 7 This PAS does not cover procurement for integration into an existing system, i.e. procurement requirements for owner/operators of a plant.

NOTE 8 This PAS will be extended into a 3-part International Standard to cover most of the restrictions expressed in the previous notes; for the planned scope of the extended standards, refer to Annex A.

2 Normative references

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.

ISO/IEC 15408 (all parts), *Information technology – Security techniques – Evaluation criteria for IT security*

ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for IT security management*

ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
access control
prevention of unauthorized use of a restricted resource, including its use in an unauthorized manner

[ISO/IEC 18028-2:2006, modified]

3.1.2
adversary
entity that attacks, or is a threat to, a system

[RFC 2828]

3.1.3
alert
instant indication that an information system and network may be under attack, or in danger because of accident, failure or people error

[ISO/IEC 18028-1:2006]

3.1.4
asset
anything that has value to the organization

[ISO/IEC 13335-1:2004]

3.1.5
assurance
performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives

[ISO/IEC/TR 15443-1]

3.1.6
attack
attempts to destroy, expose, alter, or disable an information system and/or information within it or otherwise reach the security policy

[ISO/IEC 18043}

3.1.7
attack surface
set of system resources exposed directly and indirectly to potential attack.

3.1.8

audit
formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity

[ISO/IEC 18028-1]

3.1.9
authenticate, authentication
provision of assurance of the claimed identity of an entity

[ISO/IEC 19792]

3.1.10
availability
property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 7498-2]

3.1.11
commercial off-the shelf (COTS)
items which are manufactured and distributed commercially for multiple usages and/or customers; may be tailored for specific usage

NOTE COTS is in contrast to custom products designed entirely and uniquely for the specific application.

3.1.12
compromise
unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion.

3.1.13
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-3]

3.1.14
credentials
means of proving that it is the one who claim to be, the abstract can be an IT account to access an information service or resource

[ISO/IEC 24760]

3.1.15
demilitarized zone (DMZ)
security host or small network (also known as a screened sub-net) inserted as a 'neutral zone' between networks
[ISO/IEC 18028-3]

NOTE It forms a security buffer zone (ISO/IEC 18028-3).

3.1.16
denial of service (attack)
attack against a system to deter its availability

[ISO/IEC 18028-4]

3.1.17
event
occurrence in a system that is relevant to the security of the system

[RFC 2828, modified]

3.1.18
exposed, exposure
evident state of being vulnerable and exposed to attack

3.1.19
external
outside of, or at the external border of the security perimeter of the ICN, i.e. relating to an external organizational or public network

3.1.20
external connectivity gateway (ECG)
dedicated security gateway (SGW) at the external border of the security perimeter of the ICN, typically with additional functionality to meet specific requirements, i.e. for the connectivity of external devices

3.1.21
external network (EN)
network external to the ICN and either part of the organization to which the ICN belongs, belonging to a third party or public, i.e., the Internet

3.1.22
forensic
post-incident effort to explain an event in a formal and verifiable manner to attribute responsibilities in a consecutive and logical manner

3.1.23
gateway, security gateway (SGW)
point of connection between networks, or from a network to subnetworks and external networks, intended to protect a network or subnetwork according to a specified security policy

[ISO/IEC 18028-3, modified]

NOTE A security gateway comprises more than only firewalls; the term includes routers and switches which provide the functionality of access control and optionally encryption (ISO/IEC 18028-3).

3.1.24
harden, hardening
removing unnecessary functionality to reduce physical, logical and/or organizational vulnerabilities

3.1.25
human-machine-interface (HMI)
equipment function designed to present information output to, and to accept information input from the operator to make a human, as operator, integral part of a process

3.1.26
incident
security event, or a combination of multiple security events, that constitutes a security

3.1.27
industrial control network (ICN)
network connecting ICS equipment; different ICNs may coexist within one plant and may be connected to remote equipment and resources outside the plant

3.1.28
industrial control system (ICS)
system consisting of computing and industrial control hosts, devices and equipment, that are integrated together to control an industrial production, transmission, or distribution process

NOTE In the context of this PAS, the term ICS stands for automation systems in general, including supervisory control and data acquisition (SCADA).

3.1.29
insider, inside, internal
(entity) inside the security perimeter; insider is an entity authorized to access system resources

NOTE An insider attack refers to use of system resources in an unauthorized manner.

3.1.30
integrity

safeguarding the accuracy and completeness of information and processing methods

[ISO/IEC 21827]

NOTE Integrity may apply specifically to data (data integrity) or to the integrity of the operational ICS as system integrity.

3.1.31
intranet
computer network, especially one based on public network technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders

3.1.32
intrusion
incident in which an unauthorized entity, i.e. an attacker, gains or evidently attempts to gain, access to restricted system resources

[RFC 2828, modified]

3.1.33
intrusion detection
security service that monitors and analyses system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner

[RFC 2828]

3.1.34
(cryptographic or physical) key
device, media or plaintext associated with authentication or cryptographic methods or access control privileges.

3.1.35
log, logging
gathering of data on information security events for the purpose of review and analysis, and ongoing monitoring

[ISO/IEC 18028-1]

3.1.36
malware
malicious software, such as a virus or a trojan, designed specifically to damage or disrupt a system

[ISO/IEC 18028-1]

3.1.37
(counter-) measure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an incident by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

[RFC 2828]

3.1.38
message
ordered series of octets (or bits) intended to convey information

[ISO/IEC 2382, modified]

3.1.39
monitor
observe real-time actions and events to provide evidence about what was observed

[ISO/IEC 13888-1, modified]

3.1.40
non-repudiation
property of an action that permits repeated subsequent proof that the action was performed by, or originated from, a given actor

[RFC 2828, modified]

3.1.41
owner/operator
business enterprise responsible for operating an ICS or SCADA system

3.1.42
partition, partitioning
delimited physical or logical zone to allow or deny access to resources, subject to access rules and control mechanisms

[CCOPP v0.5, modified]

NOTE A partition has a clear border with other partitions. The security policy of a partition is typically enforced by a combination of mechanisms both at the partition edge and within the partition. Partitions can be hierarchical.

3.1.43
perimeter
boundary of a network partition or zone, typically protected by mechanisms according to security policy or specified access control rules.

3.1.44
physical access gate (PAG)
physical access point to control the authorization of, for example, personnel and equipment when entering or leaving the security perimeter of the plant and/or a physical ICS partition

3.1.45
plaintext
human or machine readable and intelligible data, i.e. data input prior to transformation by encryption, or data output by decryption

[RFC 2828, modified]

3.1.46
plant
facilities, typically with a physically protected perimeter, hosting the physical process, the ICS and its ICN

3.1.47
privilege
right or permission expressly granted to a single or specified group of user(s) or device(s) to perform specified actions, in specified roles and associated to established identity

3.1.48
proxy (server)
computer process that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client

[RFC 2828, modified]

3.1.49
real-time
referring to the response time of computing devices as being so short that it seems to be immediate and without delay

3.1.50
redundancy
duplication of security critical components of a system with the intention of increasing availability of the system

NOTE While redundancy increases the availability, for example, of a communication channel, its side-effect generally is an increase in vulnerability.

3.1.51
residual risk
risk that remains after countermeasures have been applied

[RFC 2828]

3.1.52
risk
combination of the probability of an event and its consequence where probability is the extent to which an event is likely to occur

[ISO/IEC Guide 73:2002]

NOTE Consequence is the harm to assets.

3.1.53
secure, security
a product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats

[ISO/IEC/TR 15443-1]

3.1.54
security centre
trusted resource for monitoring, patching, updating, handling signature and alert information relative to the security maintenance of the ICN; an external security centre is located outside the ICN security perimeter

3.1.55
(information) security management system (ISMS)
that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve organizational security

[ISO/IEC 27001, modified]

3.1.56
security measure
(security) measure against possible breach of security of a protected system

3.1.57
security policy
set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

[RFC 2828]

3.1.58
security relevance/relevant
item, i.e. action or event, that could result in a breach of security

3.1.59
security violation
act or event that disobeys or otherwise breaches security policy

[RFC 2828]

3.1.60
strength of function
quality of a security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms

[ISO/IEC 15408-1, modified]

3.1.61
trust, trusted
expectation that a partition, host or device will behave in a predictable manner for a specific purpose under specified operating condition and subject to explicit security policy

3.1.62
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[RFC 2828]

3.1.63
user
person, organization entity, or automated process that accesses a system, whether authorized to do so or not

[RFC 2828]

3.2 Symbols and abbreviated terms

COTS	Commercial off-the-shelf
DMZ	Demilitarized zone
ECG	External connectivity gateway
EN	External network
GPH	General purpose host
HMI	Human-machine-interface
ICS	Industrial control system
IDS	Intrusion detection system
ISMS	(Information) security management system
O/S	Operating system
PAG	Physical access gate
ICN	Industrial control network
PSM	Portable storage medium
SED	Stand-alone external device
SGW	Security gateway