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]