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 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 It also gives information on projects, withdrawn and replaced publications.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

4 Introduction and compliance

Use of IT security methods and standards have become common place in the office environment in the form of the ubiquitous code of practice for information security management (ISO/IEC 27002, previously known as ISO/IEC 17799), for operational security, and the evaluation criteria for IT security (ISO/IEC 15408), for product development.

Now the internet and wireless networks have arrived on the shop floor. Security problems in automation systems are increasingly making headlines in the specialized press; but commonly acknowledged practice and related standards are lagging, and this despite the higher stakes involved in automation systems, with possible physical production losses and impact on health, human life and environment.

As has previously occurred in the operational security in the office environment, this PAS is an initial effort to provide guidance for the operational security of automation systems.

However, the methods and standards from the office environment cannot be easily applied to automation systems. A study of EWICS [15][1] has shown that the widely used ISO/IEC 27002 would have to be extended considerably to be applicable to industrial control systems. While 189 items have been judged applicable to very applicable, 85 % or 45 % have been found to require additional guidance.

This PAS contains good practice identified by practitioners based on their practical experience but developed independently of ISO/IEC 27002.

NOTE While it may be desirable to harmonize the structure and vocabulary of this PAS with ISO/IEC 27002, this has not been done at this time.

This PAS is intended to fill the presently existing void while further efforts are planned to enhance the guidance in a future edition of IEC 62443 as outlined in Annex A.

Compliance to the policy of this PAS is a local matter. It may be stated in reference to all provisions of the ICS policy or to part of it or to a customized version of it.

Certain measures of the policy may not be applied because they are not applicable at a given time for a given configuration in a given security context. The policy allows for this modularity and customization.

Also, depending on the specific ICS, it may be deemed necessary or desirable, for example, from a risk/cost trade-off perspective, not to implement certain measures as prescribed by the policy. By the nature of security, this may only be done temporarily in application of ICS policy using its exception management provision.

5 Principles and reference models

5.1 General

This PAS describes good practice in terms of technical and organizational security measures for the protection of the ICS and its industrial control network (ICN), including generally existing ICN subnetworks.

This clause explains the underlying reference models.

———————

[1] Figures in square brackets refer to the bibliography.

The users of this PAS should customize these models for their specific application, in order to apply the provisions of the security policy to their specific requirements.

The advice of this PAS may need to be complemented by other models and related policy, i.e. threat-risk assessment, general security policy, and ISMS.

5.2 Threat-risk model

5.2.1 Overview

A general security related threat-risk model is shown in Figure 1. From the figure can be read:

- threats are using vulnerabilities of the ICS;
- without counter-measures they may represent intolerable risk (to the assets);
- generally counter-measures are required to minimize risk (to the assets).

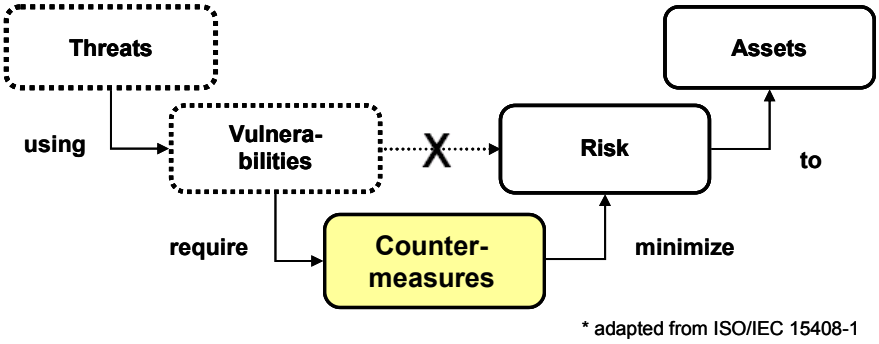


Figure 1 – Threat-risk relationship

Counter-measures are widely available, as general processes, detailed procedures and sometimes in detail specifications.

This PAS will provide counter-measures as processes, and this in the form of a proposed policy.

5.2.2 Threats

Threats are possible security-related unwanted events causing damage, i.e. monetary loss. Events that have some likelihood to occur in an ICS are:

- attacks by vandals and terrorists;
- ICS failure following a security event;
- denial of service attacks;
- breach of confidentiality, for example, disclosure of production information;
- breach of the law;
- undesirable event through acts of God, for example, extreme weather conditions like a storm or tornado.

Other events could be added that may be specific to a particular organization.

Typically, occurrence of such events would be reported to management, the speed of reporting, related action and the level of management involved being a function of their severity.

Such an event, also known as security incident, may be thought of as a newspaper headline.

5.2.3 Risk

Risk is defined in ISO/IEC Guide 73 as a "combination of the probability of an event and its consequence", as the damage, or consequence of a security incident. The occurrence of an incident may give rise to one or more consequences and may also trigger other events.

Damage that may be suffered in an ICS includes

- loss of revenue;
- unanticipated costs;
- inability to carry out some or all of a business;
- loss of the monetary value of buildings and contents;
- safety incident;
- fines due to violation of legal requirements such as emission control;
- consequences due to violation of regulatory requirements such as GAMP 0;
- customer dissatisfaction;
- adverse press coverage;
- court action against an employee or the business itself.

It is a fact that protection efforts require monetary efforts for technologic, physical and organizational measures. Therefore, the consequence of an adverse security event generally needs to be expressed in monetary terms.

The risk to the assets of the ICS requires to capture the value of the assets and their unsecured exposure to attack. This is usually very difficult and subjective, for example, when considering as a consequence a loss in the reputation of an organization.

5.2.4 Threat-risk assessment

Threat-risk assessment (TRA) leads to the evaluation of risk and its correspondent assets-at-risk, threats and vulnerabilities. TRA is a prerequisite to the selection and detailed specification of protection measures.

TRA, in particular with respect to electronic attack on computer systems connected to unsecured or untrusted networks, are at this time not amenable to mathematical-statistical analysis, i.e., malicious human attacks are purposeful and do not have the statistical property of random failure events. Thus extrapolating from historical data (as generally possible with random failures) cannot predict the future probability of human attack. For this reason, the likelihood of security-related occurrences may elude a purely statistical approach forever.

While there are many TRA models available, none has been widely accepted. Quantitative methods are misleading. Generally, security risk is assessed by in-house experts or consultants, followed by evaluation against the ICS owner/operator's risk criteria.

Because of the foregoing, this PAS does not propose TRA methods.

5.2.5 Risk treatment, acceptance and communication

After their assessment, risks generally will be found unacceptable without risk treatment.

Risks are treated using such measures as those proposed by this PAS, other measures that may be indicated as prerequisites in this PAS, and still others that are not mentioned in this PAS and that may be judged necessary by the owner/operator of the ICS, a regulator or the legislator.

Security measures should be

- effective, efficient, and strong enough to withstand identified threats;
- predictable with respect to the effort for establishing them;
- easy to install and to use;
- free of retroactive impact on the existing manufacturing process;
- ideally maintenance-free.

Most of the requirements of this PAS will allow for options differing by the amount of invested effort and obtained level of protection, to suit acceptable risk. Strength of measures should be balanced such that achieved protection by one measure may not be weakened by lack of protection of another measure.

Measures have to be reasonably complete, that is not leaving security holes. In concert, measures should mutually independent and preferably supportive of each other. Special care shall be given to assure that measures do not impede each other.

Measures are costs. Therefore, chosen measures need to be balanced to yield a cost-effective solution. If an organization cannot afford the cost, this may require an optimization process, including change to ICS configuration, limitation of communications and complementary organizational measures.

Finally, risk has to be accepted by the stakeholders and communicated to those involved prior to the implementation of measures and at every major change.

NOTE The foregoing, and this PAS, do not cover formal establishment of trust which requires security evaluation using acknowledged criteria and methodology, for example, ISO/IEC 15408 and/or ISO/IEC 27001.

5.3 Security life cycle

The provisions of this PAS are based on a security life cycle model, shown in Figure 2.

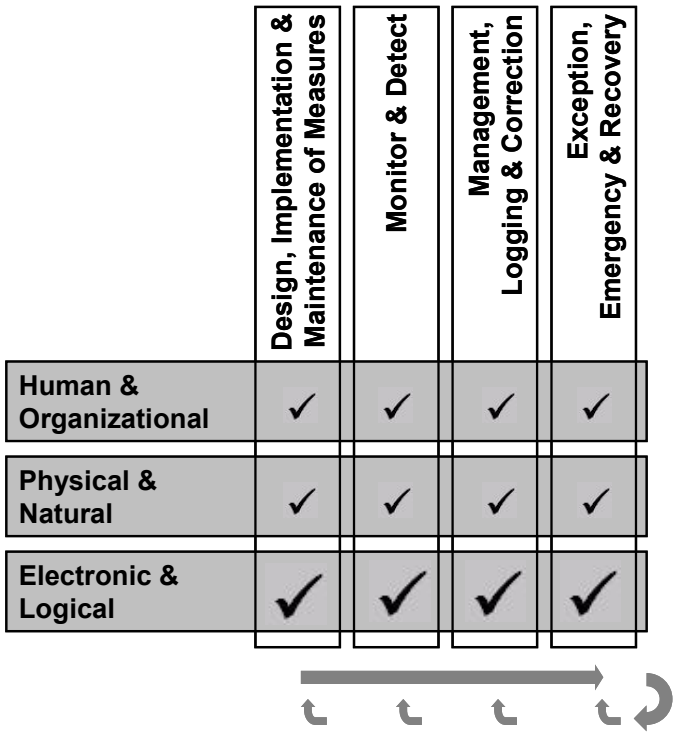


Figure 2 – Security life-cycle

The following three areas of threat and (counter-)measures should be addressed when securing an ICS.

- Human and organizational threats and measures, i.e., malicious insiders and inadequate personnel supervision.
- Physical and natural threats and measures, i.e., malicious outsiders and physical access control.
- Electronic and logical threats and measures, i.e., e-mail and anti-virus programs.

As the sizes of the check-marks in Figure 2 suggest, this PAS is mainly concerned with electronic and logical aspects.

NOTE Where a specific application-oriented life cycle is required (for example, safety life cycle) this life cycle management procedure should integrate the IT-security aspects of this PAS.

The model suggests four (4) areas of attention:

- design, implementation and maintenance of (risk containment) measures, including update and patch management;
- monitoring of the thus created and maintained security system, i.e., to detect any intrusion;
- management of the system, including log preservation and corrective actions as long as the intrusions are manageable;
- exception, emergency and recovery management when more serious incidents happen, including contingency management of worst-case scenarios.

As the straight arrow suggests, these four (4) logically sequential areas are logically sequential in concept, and may be entered sequentially at least initially at the start-up of an ICS after securing it.

However, it is important to recognize that – unlike traditional engineering disciplines – the nature of security engineering is a never-ending process. This process requires that all areas are continuously or periodically re-entered to adapt the ICS to the ever-changing technology and threat environments.

5.4 Policy

5.4.1 Overview

Policy is a collection of generic security principles and measures. Measures are grouped according to security aspects which relate to general well-acknowledged security concepts.

The measures proposed by this policy remain generic to allow for scalability, freedom of choice of appropriate available technologies and future evolutions.

Policy is hierarchically structured into four (4) policy levels, as shown in

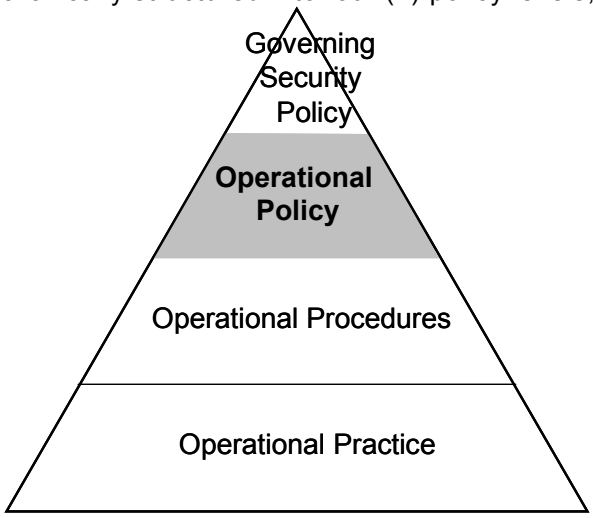


Figure 3. This PAS concentrates on proposing operational policy which generally has the character of processes. Operational policy should be understood within the complete policy framework.

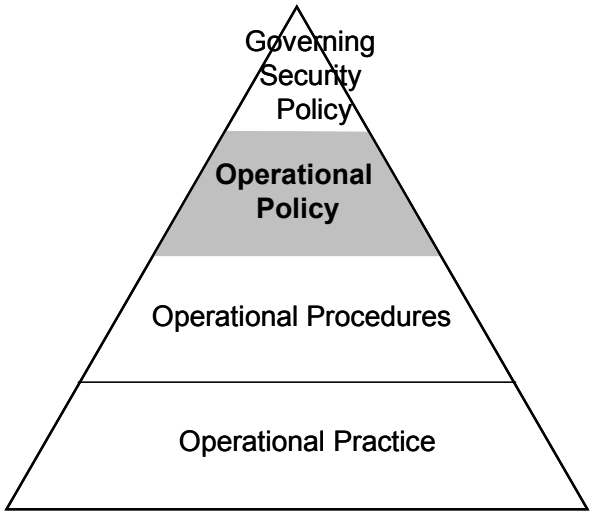


Figure 3 – Policy levels

5.4.2 Governing security policy

The policy at the top level of an organization mandates the security program and sets the direction. It states the organization's overall security objectives.

The policy statement of top management should be circumspect enough to remain pertinent and accurate through changes in the structure of the organization, changes in system and security technology, and changes in the kinds of security threats. By being circumspect, the policy can be stable and will need to be rewritten only when the organization's basic position on security changes. However, the policy statement is also unambiguous; it clearly identifies what is required.

The organization’s top-level security policy proposes general areas of responsibility and accountability for organizational areas.

NOTE For example, the policy may define the relationship between the corporate IT department and ICS management and identify their respective responsibilities. The policy may differentiate security objectives of the control system from those of the corporate network, for example, maintaining confidentiality may be a top

consideration of security for the corporate network, whereas maintaining continuous operation may be a top consideration for the control system.

In addition, the organizational security policy may identify particular standards and regulations that apply to the organization as a whole.

Management should communicate the security policy throughout the organization so that all employees understand it and may also indicate the consequences for policy violations.

Security policy at this level is reviewed periodically. Periods may vary as seen appropriate by management, more frequently in the initial phases after introduction.

This level of ICS security policy is reflected in Clause 7.

5.4.3 Operational policy

Operational policies are developed at lower levels of the organization to specify how the provisions of corporate security policy are implemented in respective organizational areas.

They define what a specific organizational area will do to achieve the objectives of corporate policy. They govern security procedures at the level below.

Procedures should address all applicable life-cycle phases of a security program, from the viewpoint of the specific organizational unit:

- system design;
- procurement;
- process operation;
- system maintenance;
- personnel;
- audit.

Policy at this level typically is reviewed periodically and at certain occasions, for example, whenever a new business process is adopted, an existing one is changed, or a business is removed.

This PAS focuses on ICS operation and maintenance. It does not provide guidance on issues like wireless devices and sensors, personnel, subcontractor policy and procurement.

The corresponding level of ICS security policy is reflected in 7.3.5.5 which covers the areas of

- integrity management;
- logical access management;
- physical access management;
- partition management;
- availability management;
- administration, audit and emergency management;
- external access management.

5.4.4 Operational procedures

Procedures should be established by an own/operator to implement the operational policy proposed by this PAS and assign their ownership and accountability for their performance, review and updating.

Operational procedures define how to perform operational policy. They define activities and may refer to relevant methods and references, i.e., standards.

Policy at this level is reviewed whenever operational policy is adopted, modified, or deprecated.

The subclauses of 7.3 will touch upon certain points which should be covered by procedure.

NOTE The procedures include a procedure by which the other procedures may be changed.

5.4.5 Operational practice

Operational practice should contain specific measurable requirements and detail the procedures by providing specific practices of the owner/operator. As these are even more specific to the organization and organizational area, only examples may be provided by this PAS.

Policy at this level is changed periodically with global infrastructure governance plans and technology changes. This is very transient and subject to revision at about any time.

All measures should be reviewed by the specific user of this PAS and adapted to his/her specific requirements and risk situation.

5.5 Generic reference configurations

5.5.1 Industrial control system (ICS)

An ICS is generally composed of electronic equipment, i.e., hosts and devices, and may include networks, subnetworks and one-to-one connections, as shown in Figure 4. It typically includes an industrial control network (ICN) and its connected equipment and subnetworks, and, in many cases, via connectivity to external networks, external hosts and devices.

A present day's ICS typically uses external communications to access, and to be accessed from, external resources, as shown in Figure 4.

- ICS internal devices and operators may need to access external resources, for example, for updates or control information.
- ICS external operators and devices may access the ICN, for example, for diagnostic, maintenance, manufacturing and/or control purposes.

NOTE On-site connection of external equipment brought into the plant by maintenance personnel is considered as external communications.

External communications may be used to connect the ICN with systems, hosts and devices such as:

- external security centre(s);
- external manufacturing and management support system(s);
- stand-alone embedded device(s);
- interactive remote access console(s)/host(s);
- remote control console(s)/centre(s);
- portable engineering computer(s);
- portable storage medium/media.

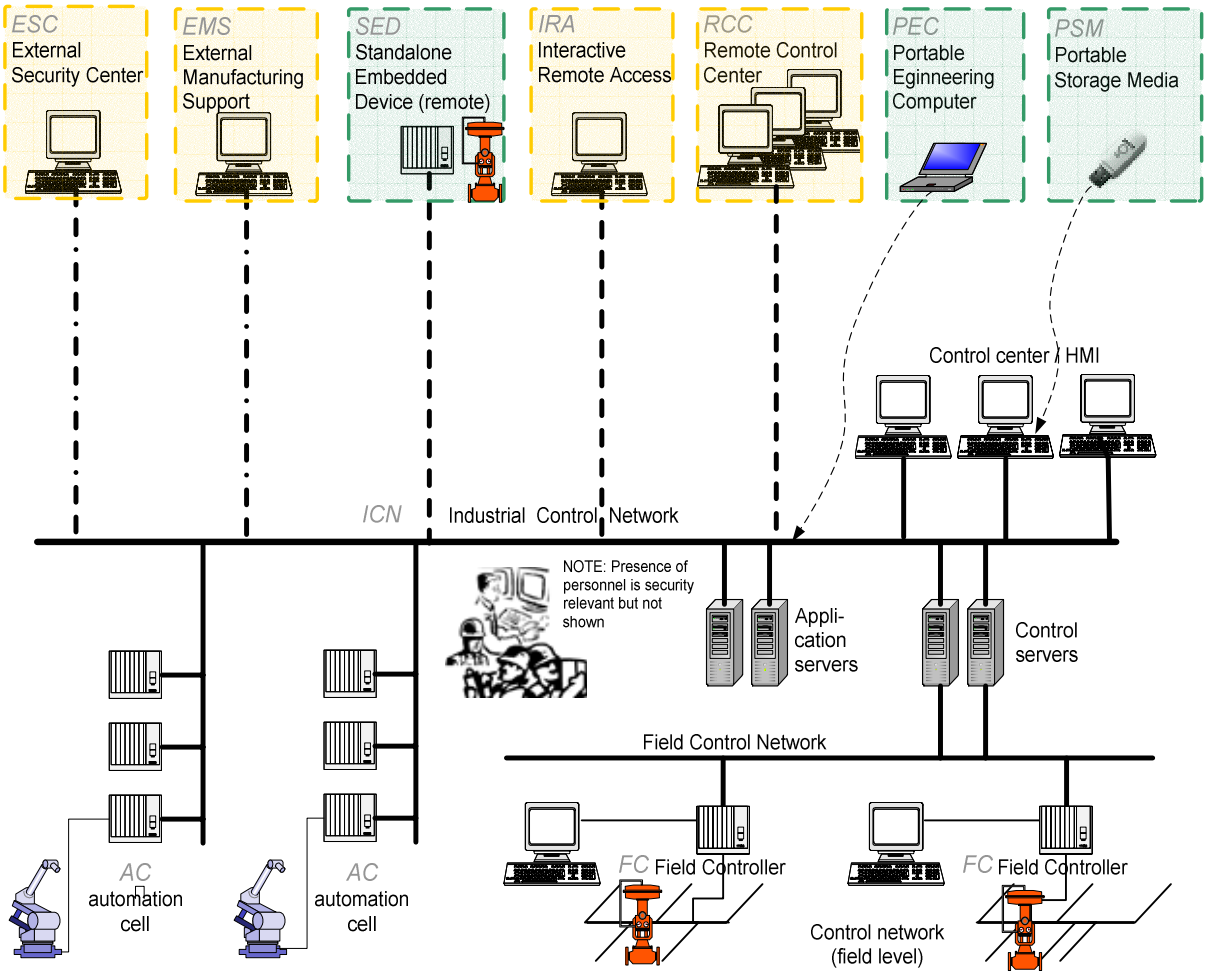


Figure 4 – Industrial control system (ICS)

5.5.2 Industrial control network (ICN)

The ICN may be built by integrating devices of great diversity, including

- hosts, proxies, gateways, hubs, routers;
- IT peripherals;
- process instrumentation, actuators, transducers, etc.

ICN hosts may function as application servers, control servers and other specific human-machine-interfaces.

The ICN connects directly or indirectly to dedicated networks, i.e., automation cells and/or field device networks.

Except for very low-complexity installations, many of these hosts and devices are connected through networking equipment and cabling to form an ICN. The ICN may include directly or indirectly connected dedicated networks, in particular automation cells and/or field device networks.

Also part of the installation are devices which contain processing and storage resources, and which are only temporarily part of the installation. Particular consideration should be given to devices brought in and out of the plant, such as lap-tops or portable memory.

5.5.3 Generic ICS host (GPH)

This PAS may be applied to hosts which may resemble to the generic ICS host (GPH). The GPH configuration in Figure 5 shows its essential components:

- the CPU with internal components such as mass storage and interfaces;
- the operator console with input device and display;
- an interface/drive to read external storage media such as a USB-stick and floppy disks;
- the interface and cabling to a control/field device;
- the interface to the ICN.

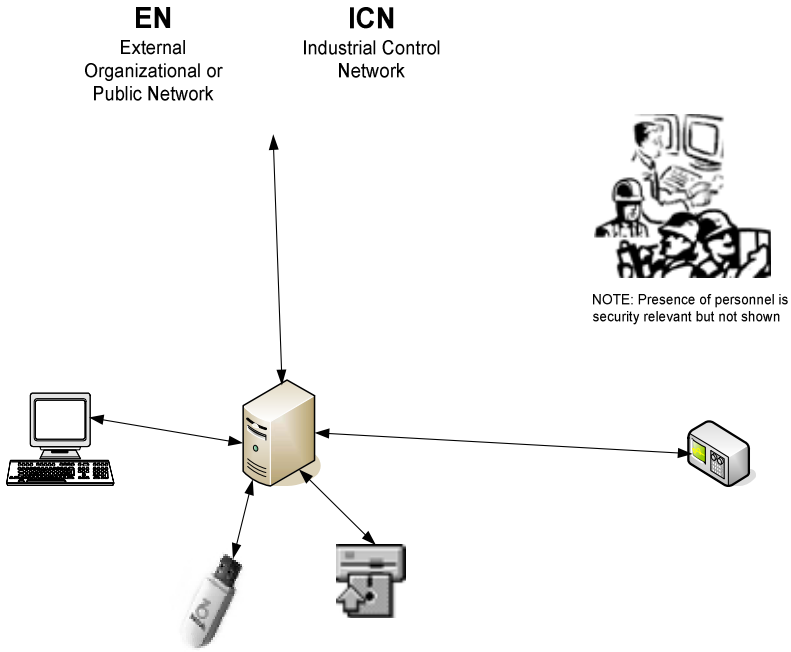
The GPH may also represent a simple ICS which does not contain an ICN. Such a system may then be connected to

- an external public network such as the Internet;
- an external organizational network.

The GPH reference configuration shown in Figure 5 will serve for conceptual reasoning about

- the most simple ICS without an ICN;
- individual hosts within an ICS when considered as stand-alone elements;
- any programmable/programmed device as a component of an ICS in general;
- interface and cabling to an external network such as the internet or a corporate network.

Expressly noted here and in other figures is the presence of humans. Humans are part of virtually any system, even if only for remote maintenance or command, and constitute the main cause and driving force of threats.



NOTE 1 There may also exist wireless connections, for example, in replacement of the cabling to network or devices.

NOTE 2 The host configuration shown in this figure is only an illustrative example and not intended to prescribe a certain network topology.

Figure 5 – GPH reference configuration: Generic ICS host with external devices

5.6 Protection models

5.6.1 Integrity and access protection

The basic security principles of integrity and access management can be shown using the simple GPH reference configuration (see Figure 5).

Figure 6 visualizes protection zones applied to the GPH. It shows that threats, i.e., from the ICS and its environment, may be stopped at the physical boundary of a room, the physical boundary of a cabinet, or the electrical boundary of a CPU and its interfaces.

A logical boundary around the GPH may be created by the integrity measures of hardening in terms of OS, applications and services configurations as expressed by the dashed circles in Figure 6.

Hardening of a transmission cable may be done by physical means for short distances but generally needs to be done by cryptographic means for longer distances, both shown as dashed lines in parallel to the cable.

Integrity and access control measures apply in a generic fashion to scenarios where

- an ICS internal devices and operators may need to connect to the ICN;
- an ICN is connected to other ICNs and/or subnetworks.

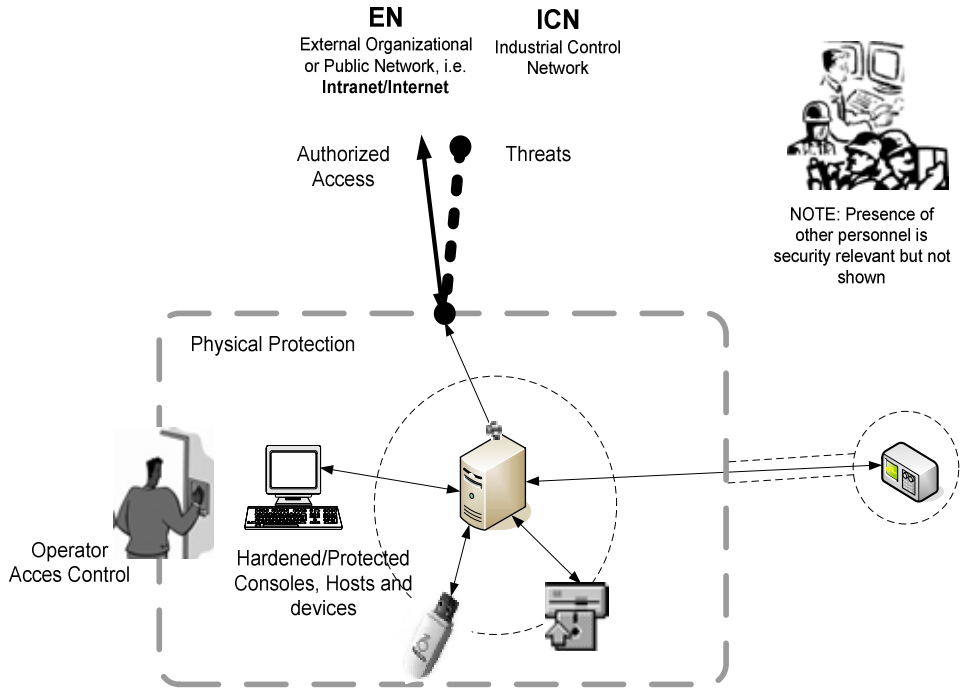


Figure 6 – Device protection: Hardening and access management

5.6.2 Protection of partitions

The architectural security concept of partitioning is based on the assumption that the industrial network can be structured into separated topological security partitions. On the same level, different partitions may be interconnected by some backbone network, i.e., the main ICN, where each partition should have a single entry point to the backbone.

Partitioning considerations apply primarily to

- the ICN itself;
- ICN subnetwork partitions;
- ICN special networking partitions, i.e., SGWs in a DMZ configuration.

NOTE The ICN is defined by the fact that it is itself partitioned off an external network (EN) and generally protected by its external connectivity gateway (ECG) from to external devices and/or networks.

Additionally, special (non-network) partitions may be created within physical hosts and devices, by providing suitable access control to protect, for example:

- a host or device by itself from ICN threats;
- the kernel of operating systems and its network services from applications and tools;
- critical applications from less critical ones;
- security monitoring and administration applications from control applications.

The prime protection measure for high security networks are

a) hierarchical or staggered partitioning;
b) stringently narrowed interface functionality (down to the minimum required, for example, usage of a limited set of functions/addresses);
c) stringent access control measures (for example, application of a specific permission scheme, blocking of unauthorized modifications, specific denial of service counter-measures).

NOTE Network or network partitions involving safety applications according IEC 61508 (IEC 61511), emission monitoring applications according to local legislation and quality control applications according to industry agreements such as GAMP 0 need particular attention and may be treated as high security networks.

In hierarchical partitions each subordinated partition receives, by the fact of partitioning, added protection and "defence-in-depth" because the protected border of each subordinated network constitutes an additional line of defence.

NOTE 1 The network outside of a partition, even if still within the ICN may be considered “untrusted with exceptions” with regard to network traffic types and volumes as well as user intentions and capabilities.

Successful additional protection on the attack path from the outside to the inside of the network does not rely on border defence alone but also on detection and reaction.

Figure 7 visualizes an example of the defence in-depth concept provided by hierarchical partitioning. It shows that threats, for example, from the internet, are already stopped at the border of the organizational external network. However, ICS security policy considers this organizational external network as untrusted and requires threats to be stopped at the ICN boundary as well.

Should an attack not be stopped at the ICN boundary, the attacker must overcome further measures at the individual devices and servers as well as at the border of the critical automation and field control networks. By this staggered approach, combined with other appropriate measures, the owner/operator of the plant is assured that within all reason the ICS is suitably protected against attack.

Within the ICN, any subnetwork partition is protected by an SGW at its boundary. Likewise, devices are protected by some security functionality which is indicated in Figure 7 by the dashed circle around a device.

It should be remembered that, depending on threat-risk analysis and other specific owner/operator requirements, reasonable subsets or supersets of partitioning and related measures may exist.

NOTE Any security policy should require balance of the strength of measures such that required protection of one access channel may not be circumvented by lack of protection of another channel. Therefore, the logical partitioning explained above should be complemented by adequate physical protection including policy controlling the introduction of portable devices into the plant and its partitions.

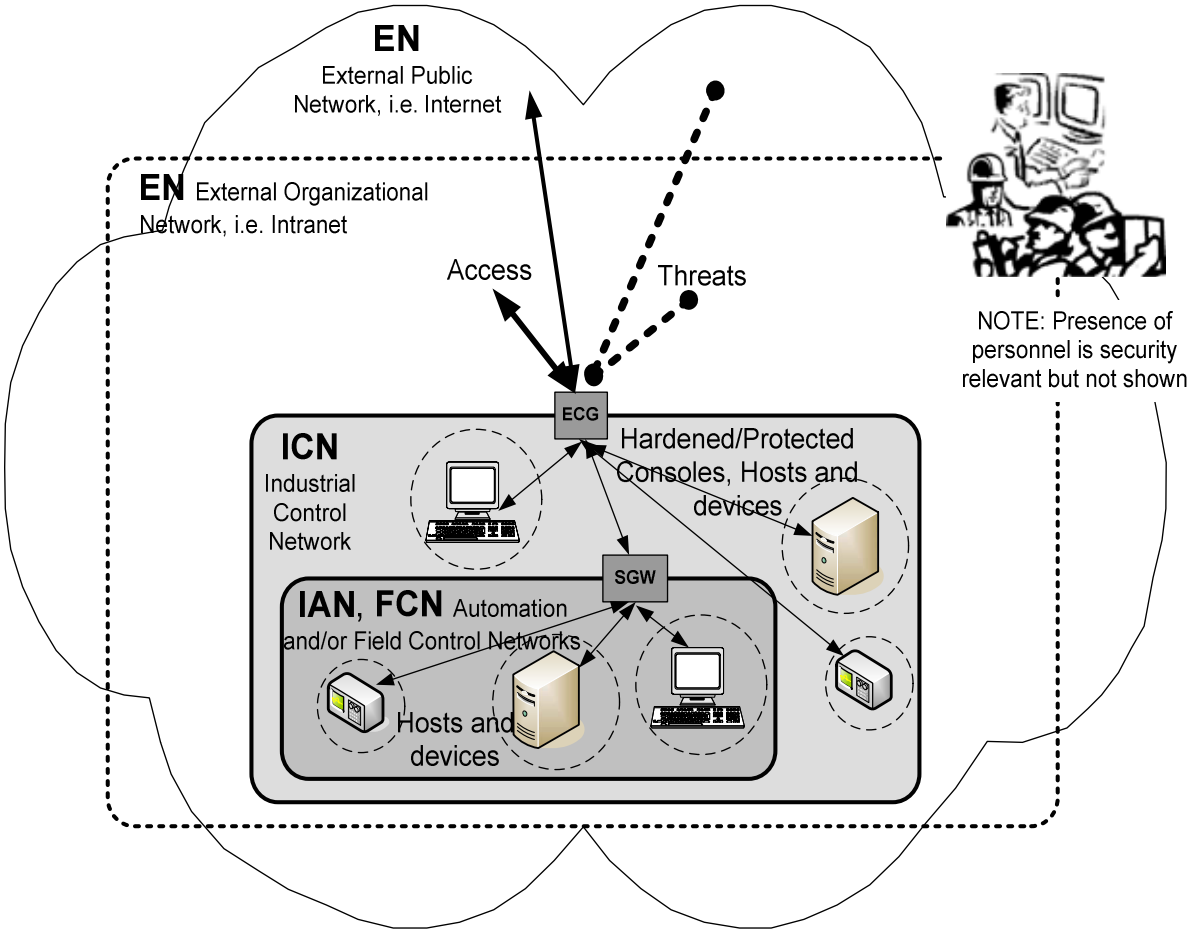


Figure 7 – Defence-in-depth through partitioning

Application of the defence-in-depth concept shown in Figure 7 to a sample scenario (adapted from Figure 4) yields the ICS partitioning example in Figure 8.

In this protection model the perimeter of the ICN is protected by an external communication gateway (ECG) and a physical access gate.

The ECG is a dedicated security communications gateway (SGW) with additional functionality to meet the requirements of specific policy, i.e., for external devices.

The physical access gate (PAG) is the physical access point by which a device has to transit when brought in or out of the security perimeter of the ICN to make sure that the ICS security policy is not being violated, for example, by transferring out confidential information or bringing in malware.

There may be additional partitions ranging from subnetworks to specific hardened devices being considered as a partition.

Examples:

- a protected control network host;
- an upper/lower level control network concept;
- network within the ICN containing all hosts with general purpose operating systems;
- specific hardened devices (i.e., hosts) where the partition equates one device; in this case, the protection perimeter is established by hardening.

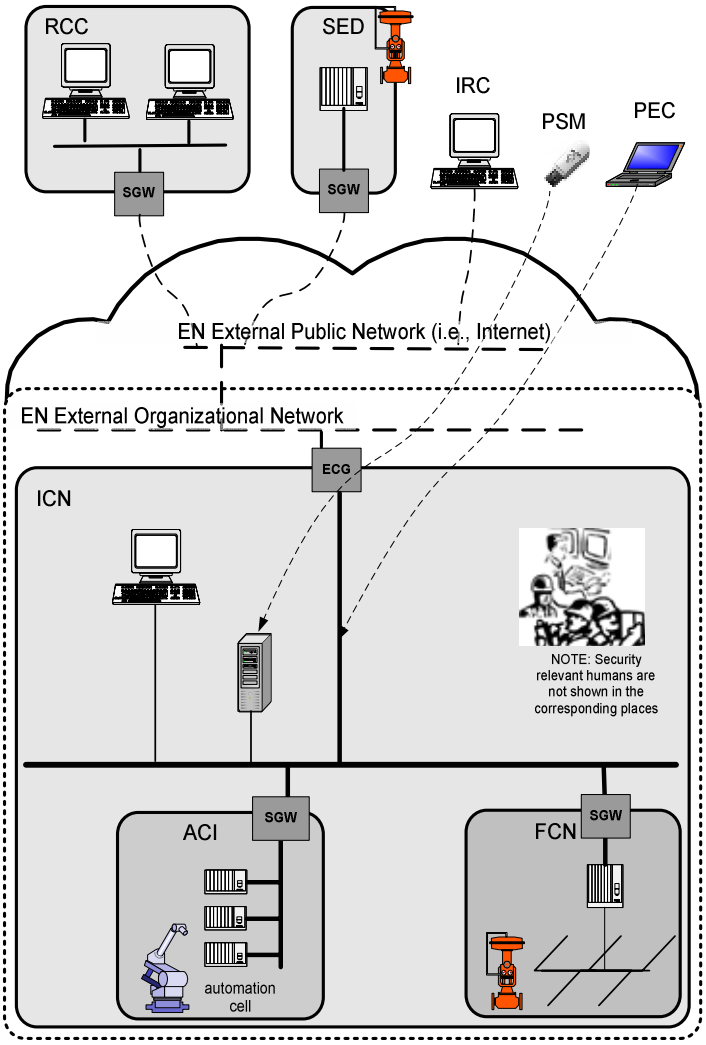


Figure 8 – Example: ICS partitioning

5.6.3 Generic external access protection

Any external network is, from the perspective of the ICN, untrusted with respect to network traffic types and volume as well as user intentions and capabilities. Therefore, this PAS describes separate network protection measures for the external border of the ICN which go beyond the measures for internal networking.

Hosts or devices may attempt to use generic external access which typically means unprotected internet services like browsing, e-mail and file transfer. Vice versa, generic external services may try to connect to unprotected generic services of the ICN.

There are two (2) components within the ICS which may respond to, or request, generic external access (see Figure 9):

– communications connectivity including interfaces, protocols and services into/ out of the ICS, at the ECG;

– internal correspondent equipment and applications inside the ICS.

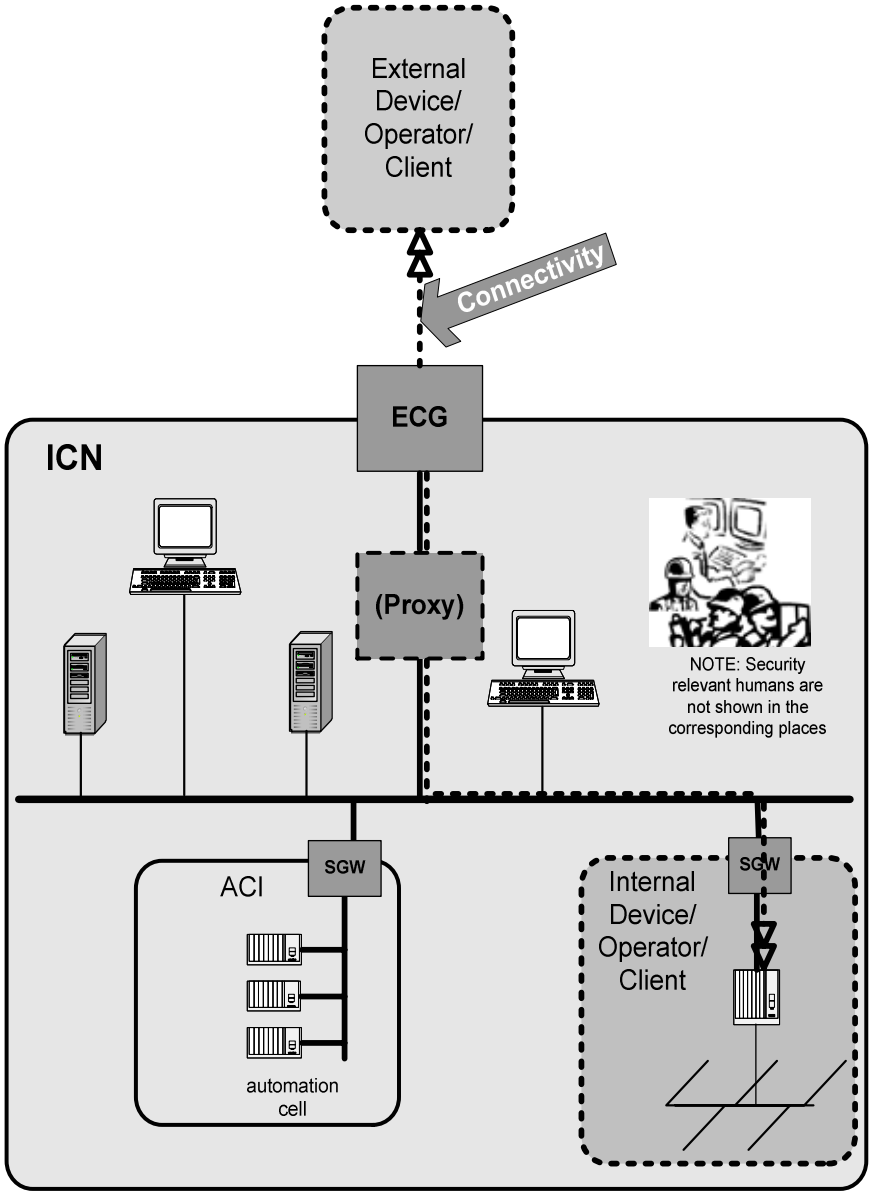


Figure 9 – Generic external connectivity

Internally, the correspondent may be the source/destination equipment communicating with the external network direct or through intermediate proxies, or a human operator.

Externally, communications partners may range from trusted to suspect.

NOTE Generic external access does not include specific industrial control external clients which will be dealt with in 5.6.4.

Established generic external access and new requests for this type of connectivity should be questioned for security reasons. For example, is it absolutely necessary to provide general web access from within the ICN?

Even for specific communications with trusted external partners and associated confirmed business requirements, the external connectivity gateway (ECG) is required to ensure that only required services are supported and external access privileges enforced.

5.6.4 External client protection

Communications to external networks shall be protected when communications to remote (external) clients is required for the operation of the ICS. ENs are, from the perspective of the ICS, untrusted (see 5.6.3). Security has to be extended to architecture, implementation, and operation of the interconnection.

External client protection measures apply in a generic fashion to scenarios where

- ICS internal devices and operators may need to access external resources, for example, for updates or control information;
- ICS external operators and devices may access the ICN, for example, for diagnostic, maintenance and/or control purposes.

ICS policy is, in particular, applicable to the protection of this external client equipment and its applications. It also deals with the important issue of equipment temporarily located outside the ICS and physically brought into the plant, to be connected directly or indirectly to the ICN, such as portable devices for maintenance and media for software updating.

The related remote access channels should typically be secured with stronger measures than those in effect within the ICS. Other than the generic external access, remote client access channels may, in addition to Internet, include specific telephone dial-up over cell-phone, radiofrequency and other public or private carriers.

One of the guiding principles for this policy is to separate the access technology as much as possible from the required security mechanisms and measures.

For external clients and proxies there is a strong relationship to internal correspondents facilitating the establishment of specific access rules and procedures on the ICN and ECG side. However, particular emphasis needs to placed on the security of the external client, which is outside the physical reach of the plan operator and therefore needs particular attention.

Higher security requirements may require communications with ICS equipment to transit through an applications proxy within the ICN as proxies give a significant security advantage.

An alternative solution is the use of end-to-end encryption with integrity protection or secure private network technology.

6 ICS security policy – Overview

ICS hosts, the ICN, internal devices and external hosts or devices shall be secured, together with their clients, as well as the access channels used by client hosts and devices to interconnect them.

This ICS security policy prescribes measures to satisfy KICN security needs when communicating with any external organizational and/or public network. These measures deal with securing hosts, devices, the ICN and communications into and within an ICS, including connected hosts and devices which are external to the plant or the ICN, and extend to high security, and potentially safety needs.

NOTE 1 The policy also allows for exceptions, subject to exception management, as well as deviation from policy risk analysis.

The proposed measures of the ICS security policy have been grouped into subclauses with the following content.

- Principles, that is policy describing generic provision which apply to all security measures that should be undertaken for the ICS and its ICN, including security prerequisites for, and specified exclusions from, policy, i.e., safety-related security requirements.
- Availability management as an issue specific to real-time networks and not prevalent in general IT (see 8.1).
- Integrity management including requirements for
  - virus and other malware protection;
  - updating and patching of software and firmware;
  - back-up;
  - file and file system integrity;
  - hardware, operating system and application hardening.
- Logical access management concerning the access to hosts, devices, media and information and includes requirements for
  - user identification;
  - user privileges, i.e., accounts and rights;
  - encryption;
  - management of the above.

NOTE This category of measures has a strong relationship to the rules that will guide the action of the security gateways.

- Physical access management providing rules for the security of physical access to rooms, cabinets, cases to secure hosts, devices and media through requirements for
  - user identification;
  - user privileges, for example, keys and other access rights;
  - management of the above.
- Partition management as the prime protection measure for high security networks. For this reason, the partitioning issue merits a separate subclause.
- External access management putting emphasis on the specific threats from external public networks.
- Administration, monitoring, and emergency management covering management and coordination issues common to above issues, providing for
  - exception management;
  - logging and monitoring;
  - emergency response.

7 ICS security policy – Principles and assumptions

Objective: to provide ICS management direction information as to what the ICS security policy covers and its position within organizational policies, other technical or organizational requirements, business requirements and relevant laws and regulations.

7.1 ICS security policy – Principles

7.1.1 ICS security policy prevails over subordinated policy except when expressly preempted.

Rationale:

Precedence has to be established in case of conflicting policy statements which may originate from different policies in effect at the plant and at locations of its contractors.

Implementation guidance:

7.1.1.1 The required level of trust between the ICS organization and the service organization should be provided by a security service level agreement

7.1.1.2 Security service level agreement should be in line with ICS policy.

Example: When the operator of the ICS and the operator of a remote control centre are different organizations or entities they may have differing IT security policies. A security service agreement may be required, for example, to address authentication measures, information containment and virus/malware threats.

Other information: refer to addressing security in third-party agreements in ISO/IEC 27002.

7.1.2 ICS security policy is subordinated to, complemented by, and in case of conflict, overridden by organizational security policy.

Rationale:

The existence of corporate policies must be respected by ICS security policy.

Implementation guidance:

7.1.2.1 ICS security policy may be expressly pre-empted from this provision; in this case substantial complements to the provisions of this PAS may be required.

Other information: refer to ISO/IEC 27002.

7.1.3 ICS security policy is subordinated to functional safety-related security policy.

Rationale:

ICS security policy does not cover safety and safety emergency functional and operational requirements which in many legislations is considered of higher if not highest importance.

Implementation guidance:

7.1.3.1 Changes in ICS security policy are subject to approval by safety management.

7.1.4 ICS security policy is complemented and, in case of conflict, overridden by local or national legal requirements.

Rationale:

Law and legal requirements (i.e., federal, state, city) prevail over organizational and technical requirements.

7.1.5 ICS security policy may be complemented and/or overridden by requirements imposed by regulatory bodies.

Rationale:

Regulations (i.e., federal, state, city, industry) may complement or override organizational and technical measures of this policy.

Implementation guidance:

7.1.5.1 ICS security policy should be reviewed, and may need to be approved by, the authority in charge of regulatory provisions, at the organization and/or the regulatory body.

NOTE Safety requirement according to IEC 61508 and IEC 61511, emission monitoring applications according local legislation and quality control applications according GAMP [16] requirements may fall under this provision.

7.2 ICS security policy – Assumptions and exclusions

7.2.1 ICS security policy does not provide for functional data availability and data integrity.

Rationale:

Data transmission real-time properties and error correction is generally part of ICS functionality and functional safety requirements and designed to correct system functionality faults and errors.

Implementation guidance:

7.2.1.1 Transmission of security relevant data should use channels that have the required data integrity properties, unless transiting by qualified industrial communications protocols.

NOTE Communications data integrity traditionally is a major security objective in IT operation. Assurance that ICS data is transmitted and received unaltered between (or among) session endpoints is assumed to be provided by industrial communications protocols.

7.2.2 ICS security policy does not provide for all comprehensive security policy.

Rationale:

This PAS is focused on ICS logical security and does not contain all the provisions which generally are part of organizational security policy.

NOTE This PAS stipulates physical security measures only if closely related to logical security measures. Other measures such as personnel security - while mandatorily required - are not covered by this PAS.

Implementation guidance:

7.2.2.1 All comprehensive security policy should be provided by organizational security policy and include, i.e. personnel, general physical and general IT security.

7.2.2.2 Generic/sector standards should be used to complement and complete ICS security policy if organizational security policy is missing or insufficient

Other information: For further information refer to ISO/IEC 27002.

7.2.3 ICS security policy does not cover procurement.

Rationale:

Procurement and, depending on risk, related security assurance and testing should be considered mandatory but not covered by this PAS.

Prerequisites and limitations:

ICS assumes the existence of an appropriate policy for the procurement and test of equipment and associated security features as required for the implementation of ICS policy.

Implementation guidance:

7.2.3.1 Procurement requirements should be adapted from the guidance and measures stipulated by this PAS.

Other information: refer to [16] .

NOTE There is presently no consensus or established practice about the extent of appropriate prescriptions for security assurance and testing of ICS security relevant equipment and devices.

7.2.4 ICS security policy does not provide for all-comprehensive operational security management.

Rationale:

Integration of the provisions of this ICS security policy into a general information system security management (ISMS) system is needed to ensure that ICS policy and measures have their intended effect over the whole operational life cycle of the plant.

Prerequisites and limitations:

A comprehensive ISMS should be implemented and include security management of its personnel, general plant security, administrative and maintenance processes and procedures, emergency management and disaster recovery as well as related awareness/education. It should include organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Other information: For further information refer to ISO/IEC 27002.

7.2.5 ICS security policy does not cover assurance of communications for mandated policy such as functional safety.

Rationale:

In case of mandated policy such as safety, and/or in case of generally accepted practice such as GAMP [16], such policy, practice and actions prevail over security policy of this PAS.

Prerequisites and limitations:

Mandated policy management, for example, safety management, shall assume the functional and security risk management associated with the use of any ICS communications channel, including the ICN.

Implementation guidance:

7.2.5.1 The availability and integrity of any channel for safety communications, within the plant as well as between the ICS and any remote control centre, is subject to safety risk management.

NOTE The lack of assurance of availability for any and all remote control centres implies that ICN channels are not assured for critical functional safety communication.

7.2.5.2 Denial of service, i.e., of an external communications channel, is a form of incident that cannot be countered direct; its effects are typically alleviated through redundancy or back-up resources.

NOTE Redundancy measures to achieve availability typically induce increased exposure and related risk.

7.2.5.3 Functional safety and other mandated policy assurance may consider the ICN and its subnetworks as “black channels” to avoid the time and expense of certifying general ICS channels to their policy requirements, and of assuring their security management.

7.2.6 ICS security policy does not cover availability of the ICN and ICN subnetworks, or any EN channel for real-time response.

Rationale:

Real-time response is a functional issue. Because of its security mechanisms may be causing additional delays real-time communications cannot be assured.

NOTE This means that real-time operation of the ICS cannot rely on the EN, ICN or ICN subnetworks. In particular, remote control centres may not respond adequately.

Implementation guidance:

7.2.6.1 Critical real-time communication should be restricted to lowest level partitions of an ICN which should have strong border protection and where virtually no logical security mechanisms are required internally.

Example: An automation cell (AC) typically will be protected at its border by a SGW of required strength. Physical access will be restricted to trusted personnel. All communications inside the cell is considered trusted.

7.2.7 ICS security policy does not cover emergency operation of the plant.

Rationale:

Emergency operation is an operational issue. Security mechanisms may not be available and therefore cannot assure communications with certainty.

NOTE This means that emergency operation of the ICS cannot rely on the ICN, ICN subnetworks or any EN. In particular, remote control centres may not be useable.

Example: This may not, from a security point of view, apply to the autonomous emergency operation of an automation cell (AC) which typically does not contain security mechanisms inside.

7.3 ICS security policy – Organization and management.

Management methods and procedures are required to operate and audit security policy.

7.3.1 Development, implementation, enforcement, review and change of ICS security policy should be the responsibility of ICS management.

Rationale:

Changes in threat, threat level, configuration, technology, etc. are unavoidable and require re-evaluation and evolution of ICS policy.

Implementation guidance:

7.3.1.1 Operational responsibility for the enforcement of ICS security policy should be assigned to a security manager who should be operationally independent with respect to ICS and plant operation.

NOTE 1 Separate responsibility for policy issues strengthens implementation and maintenance of policy, is sometimes imposed by regulators and reduces security risk.

NOTE 2 In larger organizations the security manager may be independent through exemption from operational or system administration responsibilities. In smaller organizations individuals may have to cumulate these roles.

7.3.1.2 Network equipment administration should be implemented, conducted and logged in a secure fashion.

NOTE 1 Configuration of network equipment and changes to configuration are highly security-relevant and need use of strong access control mechanisms.

NOTE 2 To avoid attack on network settings, administration should use communications channels and access privileges which are separate from production traffic and privileges, possibly a separate security management network.

NOTE 3 Administration of security and networking equipment should be feasible even when an attack or the response to an attack have the communication path for production traffic.

7.3.1.3 ICS security policy should be documented, updated for changes and exceptions, kept available and made known to concerned personnel.

7.3.1.4 All applicable organizational policies should be available to ICS management, included with ICS security policy and kept updated to allow time-constrained effective application.

7.3.1.5 Periodic awareness training on ICS policy and changes should be given to enforce its provisions.

7.3.1.6 Management should include documentation of exception, with specific business reason, as well as time of establishment, extension and termination.

7.3.1.7 Policy reviews should be performed periodically and after incidents.

7.3.2 Threat-risk management

Rationale:

Security is an issue strongly characterized by uncertainty induced by technological progress and human unpredictability and resulting in a constantly changing risk to assets. The assets of the owner/operator generally stay relatively constant. This makes the threat environment the driving factor.

Prerequisites and limitations:

This PAS does not propose a TRA method. The owner/operator shall therefore elaborate his/her risk assessment using resources other then this PAS.

Implementation guidance:

7.3.2.1 Criticality of equipment, operating systems, applications and services for the operation, management, and maintenance of the automation system should be assessed, in terms of functional availability, system integrity and data confidentiality.

7.3.2.2 The threat environment should be continuously monitored, assessed.

7.3.2.3 The strength of security measures to counter threats should be reviewed and corrected, periodically or after security events, to remain state of the art.

NOTE 1 Strength of encryption methods should be periodically adapted to technological evolution.

NOTE 2 Changes, for example, in SGW and ECG rules, in kind and level of threat should trigger configurations, technology, addition of complementary measures and equipment, etc.

7.3.2.4 Critical equipment should have an assigned technician, administrator and monitoring facility.

7.3.3 ICS safety policy and its changes should be coordinated with ICS security policy.

Rationale:

Safety and security are generally intertwined.

Implementation guidance:

7.3.3.1 ICS safety policy and its updates should be on file at and readily available to security management.

7.3.3.2 Any security-related operator action or method affecting functional safety should be subject to dual safety and security management approval.

NOTE The two-person rule ensures that actions with especially disastrous consequences can not be initiated by one person alone. This protects against intentional and incidental mal-operation. Dual approval is one of the most effective means against insider attacks.

7.3.3.3 Approval is necessary when operator action or method affecting functional safety is established, put into operation and terminated

7.3.3.4 There should be no exception to remove established dual approval.

7.3.4 ICS security policy should require logging and monitoring of security relevant events.

Rationale:

Logs serve for establishing events, sequence and assignment of responsibilities for control and audit. With respect to unauthorized actions, for example, by attack, logs may be used for forensics. Assignment of responsibility is particularly important when critical activities are outsourced.

Implementation guidance:

7.3.4.1 All security relevant automation system user activities should be logged.

7.3.4.2 All security relevant system events should be logged.

7.3.4.3 The gathered information should include event, urgency, communication service, source host, destination, user identifier, start and end time/date.

7.3.4.4 All logs and audit information should be monitored, periodically reviewed, securely stored and archived.

7.3.4.5 Logs should be stored in a central location to facilitate consolidation and analysis, to avoid exhaustion of the limited log storage space, and to avoid that an attacker can modify the logs after compromising logging equipment.

7.3.4.6 Log management activities should be logged. Only a security auditor should be authorized to delete/modify logs.

7.3.4.7 Logs and alarms should be monitored and managed to initiate conclusions and necessary actions.

Rationale:

Logs of security events need to be continuously monitored to deter malicious insider attacks and to detect attack, to be conserved for forensics after security compromise.

NOTE When compromise is detected, network connection between remote and local control centre should be disconnected until the trust is recovered. The local control centre should operate the ICS safely. In order to confirm the trust recovery, security audit should be performed.

7.3.4.8 Local legal requirements for evidence have to be respected if the logs are intended to be used as legal evidence.

Example: The following data may be logged:

- event, for example, authentication error, access violation;
- urgency, for example, emergency, alert, warning;
- communication service used, for example, service name, port number, protocol;

- source host, for example, IP address, host name;
- destination, for example, IP address, host name, URL;
- user identifier;
- start time/date;
- end time/date.

NOTE When the ICS operation is outsourced, the log is important objective evidence to assign responsibility after an accident occurred.

7.3.5 ICS security policy compliance should be audited.

Rationale:

Control of ICS policy management performance requires audit.

Implementation guidance:

7.3.5.1 ICS policy compliance audits should be performed periodically and lead to corrective action if warranted.

7.3.5.2 Audits may include security testing.

NOTE The ICS should be periodically audited for illicit/insecure equipment communications, for example, using POTS (voice-grade traditional telephone service) and wireless.

7.3.5.3 Responsibility for security audit should preferably be assigned to a qualified non-operational the security manager, possibly an external person.

7.3.5.4 If possible, separate roles for audit and administration of security measures.

7.3.5.5 Special attentions and specific audit should be granted to formal exceptions to established measures.

7.3.6 Exceptions should be managed and documented to establish acceptable accountability of individuals/devices using *ad hoc* risk management.

Rationale:

Without formal exception management these will be handled in an *ad hoc* fashion leading to loss of control over the timing, duration, and extent of the exception and loss of accountability and personal responsibility for any negative consequences.

Prerequisites and limitations:

With shared responsibility, i.e., common user accounts, the originator of a specific action in the system may not be identified while a suspected user may be able to plausibly deny involvement in an action.

As assignment may be in conflict with local labour law and/or union agreements larger scale execution management is required.

Implementation guidance:

7.3.6.1 Exception from policy should be subjected to formal exception management, including business justification, risk analysis, assignment to the responsible person.

7.3.6.2 Exception from policy should be limited to the minimum time necessary.

7.3.6.3 There should be no exception to exception management.

7.3.7 Events and alarms should be acted upon according to contingency plans in a timely manner and by criticality.

Rationale:

When a security incident occurred, it is very important to minimize the damage and to continue ICS operation, and to recover as quickly as possible fully secured operation at regular capacity.

Implementation guidance:

7.3.7.1 Contingency plans to respond to security incidents should be established and periodically updated.

7.3.7.2 Alarms pertaining to critical safety and industrial control events should be acted upon by security management, if applicable, in coordination safety management.

7.3.7.3 Incident response plans should be available for security incidents of various kind and criticalities, including continuation of plant operation and recovery of damaged equipment.

7.3.7.4 For quick and effective problem resolution, critical equipment should have documented assignment of technician, user, administrator and monitoring facility.

7.3.7.5 Critical security incident should be investigated quickly after occurrence.

NOTE 1 In some legacy applications, access to ICS devices or remote clients is using a plaintext credential protocol (for example, Telnet, FTP). In this case the access should use a secure tunnelling protocol to avoid exposing the credentials on any part of the path exposed by the public EN.

NOTE 2 Exceptions should be documented and managed.

NOTE 3 When a security incident alarm is issued by a security device, it should be notified without delay to the security management server, to the security manager. The security manager should practice the damage containment plan, i.e., the research of the affected level and safeguard of evidence.

7.3.7.6 Plans should be published to concerned personnel, together with assignment of responsibilities and associated organizational assets.

7.3.7.7 Awareness and technical training should create and maintain concerned personnel available for contingency action.

7.3.7.8 Periodic and surprise drill using divers attack scenarios should be held to evaluate the plant's capacity to cope with real event in the expected manner.

7.3.7.9 When an intrusion is detected, immediate response is necessary. This imposes the existence of adequate and up-to-date plans for security incidents that affect the functions and assets covered by these policies.

7.3.7.10 Security-induced disasters require ICS related emergency and disaster recovery plans as well as relevant recovery and contact information.

NOTE Refer to monitoring system access and use in ISO/IEC 27002.

8 ICS security policy – Measures

Objective: to reduce the risk of electronic attacks on the ICS by establishing security measures for hosts, devices and their peripheral connectivity within the ICN internally, with the ICN's subordinated networks of any level and communications with external networks.

NOTE The intended risk reduction can only be achieved if all communication paths are considered, including legacy means of communication (telephone, radiofrequency), wireless private and public networks.

8.1 Availability management

The disturbance of PCS resources by security measures may lead to downtimes, or even endanger people and the environment if safety measures are impacted. Availability

management should be used to prevent security measures from disturbing the resources required by the production process.

8.1.1 Availability of the ICN and ICN subnetworks should be assured for critical ICS operational requirements.

Rationale:

Faulty or exaggerated security measures may degrade ICN availability and prevent satisfactory ICS operation.

Prerequisites and limitations:

Real-time message availability internal to the ICN is not a security requirement but a functional issue. This PAS assumes that real-time message availability is assured by automation functions using measures such as message integrity, message freshness, message ordering and message priority assurance.

Implementation guidance:

8.1.1.1 Communications channels may require redundancy to increase availability and to avoid single points of failure.

NOTE 1 While redundancy generally increases reliability and availability, it also increases exposure and security risk, thus reducing security.

NOTE 2 Partial non-availability of communications may require use of back-up resources, reduced modes of plant operation, and worst case shut-down.

8.1.1.2 To prevent the consequences of missing availability, users and applications within a given network should be authorized to interrogate the status of the protecting equipment, for example, SGWs, and emit an alert of a related error condition.

8.1.2 Resources used by security measures should not degrade critical resources required by automation and/or safety functions.

Rationale:

Security measures should function in such a way that the process is not disturbed.

Implementation guidance:

8.1.2.1 On safety-related equipment only those security functions should be implemented which are required to secure this safety-related equipment.

NOTE Availability of any safety-related resources should not be restrained, including permission of

- special proprietary communications;
- pre-existing proprietary safety-related security mechanisms;
- appropriate ease of physical and logical access to functional safety-oriented control room operation.

8.1.2.2 Competition of security and control functions for ICN resources should be avoided or resolved, for example, by implementation of the respective functions on separate equipment.

NOTE Separation may not be possible, for example, when malware/virus scanner are deployed. In these cases it should be made sure that any implementation of security functionality on industrial control equipment is kept logically separate, i.e. using separate credentials and interrupt handlers and coordinated with industrial control personnel.

8.1.2.3 Determine, document and manage security measures that may use critical resources of control functions.

8.1.2.4 For those measures define, document, and implement resource boundaries and host behaviour in case of resource overload or overflow, including issuance of alert.

8.1.2.5 In case of conflict, priority should be given to critical industrial control functionality.

8.1.2.6 An emergency response plan for resource exhaustion should be implemented, documented and managed, and include awareness training for personnel as well as associated drills.

NOTE 1 The emergency response plan should include risk analysis and implementation of appropriate degraded operation and/or shut-down modes, reduced logging modes, and addressing alerts to the assigned user and monitoring facility.

NOTE 2 Differentiate between emergency action and its consequence on security, critical automation and safety functionality, possibly through activation/deactivation of partitions.

8.1.3 To assure functional availability of the ICN, security measures should be implemented and managed in a transparent way.

Rationale:

Implementation, update and removal of security services should not impact the functional properties of the ICS.

NOTE This means that the configuration of the ICS, any EN and remote clients can be used and remain unchanged after the integration of security.

Implementation guidance:

8.1.3.1 If installation, change or removal is causing foreseeable operational changes these have to be coordinated with ICS and/or safety management.

8.1.4 Clocks throughout the ICS should be synchronized.

Rationale:

Availability of the accurate time synchronization of devices with a sufficiently trusted source of time is required, i.e., for assurance of event sequence via logging, for consolidation and analysis.

Implementation guidance:

8.1.4.1 Establish time standard and required accuracy.

8.1.4.2 Share time with, and if not possible map, time to safety and control functions.

NOTE This includes synchronization of remote client and device clocks.

8.2 Integrity management

The system basis, reduced to the minimum of code, configuration and operation data required for the ICS functionality and security, represents the minimum attack surface to be protected against compromise.

NOTE Communications data integrity, i.e. that data is unaltered between (or among) session endpoints, is assumed to be provided by industrial communications protocols.

8.2.1 Hardware devices and interfaces configurations should be reduced to the lowest level required (hardening).

Rationale:

Generic or unhardened hardware configurations containing unused interfaces and peripherals increase the attack surface, in particular for insiders.

Implementation guidance:

8.2.1.1 Unused interfaces for operator I/O, peripherals, communication and data storage devices should be removed or otherwise made permanently inoperable.

8.2.1.2 Cabinets and slots accessible from outside that cannot be removed should be protected, i.e. physically locked.

8.2.2 Applications, O/S services and O/S utilities should be reduced to the lowest level required (hardening).

Rationale:

The risk that an attacker is able to compromise a system increases with the number of applications and services available on the hosts and devices.

Implementation guidance:

8.2.2.1 The list and configuration of applications, O/S services and O/S utilities required for the operation of the ICS should be documented.

NOTE The sets of permissible communications may depend on the formal operating state of the plant or unit, such as normal operation, declared emergency operation, or start-up/shut-down operation.

8.2.2.2 All parameters of required network services on the host and of incoming and outgoing dataflow with other hosts and devices on the ICN should be documented.

8.2.2.3 Applications, O/S services and O/S utilities not required for the operation of the ICS should be removed from the configurations and their back-up.

NOTE 1 Services receiving directed broadcasts should be removed.

NOTE 2 If not removable, applications, O/S services and O/S utilities not required for the operation of the ICS should be made permanently inaccessible to any user.

NOTE 3 A host-based SGW (also known as personal SGW) only disables and rejects communication destined for certain services but does not remove code.

8.2.2.4 Required applications, O/S services, O/S utilities and security services should present a hardened attack surface prior to being connected to the ICN.

NOTE Best practice hardening guidelines for various operating systems and applications are offered, i.e., by NIST, NSA, SANS, CISecurity.

8.2.3 Configurations and identities should be created and maintained to be reasonably unique.

Rationale:

Host configurations that are totally identical copies will represent a large attack surface and facilitate compromise, for example, through automated attack, leading to compromise of all identical systems.

Prerequisites and limitations:

Configuration diversity is creating a security gain through obscurity. This gain should be offset, for example,

- by additional cost, for example, through the administration and patch management of diverse equipment;
- by the loss of security induced by operator and administrator errors due to configuration complexity.

Settings imposed, for example, by vendors on legacy equipment, may not be available for change.

Implementation guidance:

8.2.3.1 Systems preconfigured by the vendor or cloned by the owner/operator or the system integrator should be changed from default/preconfigured and/or commonly used settings to be reasonably unique.

8.2.3.2 Change of settings should be documented, transparent for the user and protected from change.

8.2.3.3 Unique identities that have been created by the owner/operator may have to be restored after installation of patches.

NOTE Patches may restore to preconfigured default settings.

8.2.4 System and device installations, i.e. their configurations, start-up processes, maintenance and operational integrity, should be managed.

Rationale:

The system constituents and their interconnection should correspond to the desired trusted state when executed. For this purpose, system configurations need to be managed and up-dated as frequently as required from the security point of view.

Prerequisites and limitations:

In general, patches and updates should be installed as they become available. However, a security patch or update may conflict with the control system functionality, resulting in degraded or unavailable functionality or degraded timing behaviour.

The inverse may also be true, that is a control system patch or update may conflict with the security measures, resulting in degraded or unavailable security functionality.

Obviously, the automation system vendor is unable to test a patch or update on every possible control system variation, in particular on the specific ICS implementation.

Implementation guidance:

8.2.4.1 Current baseline configurations should be developed, documented, and maintained.

8.2.4.2 An inventory of the system's constituent components and operational status should be kept as back-up and archive, and protected for integrity.

8.2.4.3 Security patches or updates should only be considered after approval by the respective automation device or system vendor.

8.2.4.4 Vendor approved security patches or updates should only be installed after additional testing for and on the ICS.

NOTE Back-up, training, or development systems, if available, should be used for in-plant testing.

8.2.4.5 New applications, services and patches require a sign-off process prior to installation on the ICS.

8.2.4.6 The risk of partial system failure or deviations during or after an system installation, modification should be assessed and mitigated, i.e., after deployment of updates.

NOTE 1 A problem resolution process should be in place, including reverting to the last secure and functionally correct state.

NOTE 2 A staged deployment may be considered to retain some control capability in case of problems with the software modification.

8.2.5 Executable images, baseline and back-up of operational system, status and production information should be managed.

Rationale:

Adequate executable image integrity and back-up ensures that all essential information and software can be recovered following incident or failure, to quickly resume secure operation and to maintain the integrity and availability of systems and data.

Implementation guidance:

8.2.5.1 Back-up should periodically be taken, tested, validated, and securely archived.

8.2.5.2 Back-up should include all security and operationally required functionality parameters to enable quick recovery

8.2.5.3 Operational file system integrity check utilities should be available and installed to detect changes; tools and procedures should be available to restore exactly to the required state.

8.2.5.4 Illicit configuration changes, for example, through malware/virus infection should be prevented, and if occurring, detected to trigger alert, response and remediation.

NOTE 1 Resources of the ICS may be heavily impacted by scanning. Refer to resource availability management of this PAS.

NOTE 2 Signature-based malware/virus scanners are only effective with current signatures.

NOTE 3 Scanners should be deployed and configured only as indicated by the respective automation system vendor and to scan only designated equipment.

NOTE 4 Scanners and signatures for COTS hosts and devices that are not critical may be installed at the owner/operator's risk taking caution that scanning does not violate critical boundaries such as networked devices.

NOTE 5 COTS signatures may falsely identify certain legitimate custom application files as malware. Therefore, signatures should be tested prior to application to a specific automation system or approval be obtained by the respective automation system vendor.

8.2.6 Integrity management should include monitoring, logging and alarm escalation procedures.

Rationale:

Without integrity monitoring and alarming the owner/operator cannot demonstrate that integrity is maintained. Logging is also necessary for anomaly detection and forensic analysis.

8.2.6.1 All SGWs should be centrally monitored

NOTE Refer to logging in 7.3.4.2.

8.3 Logical access management

This ensures only authorized logical access to ICS resources according to assigned privileges.

8.3.1 Identities, addresses, keys and associated user/device credentials and rights/privileges should be assigned and managed.

Rationale:

Verification of the identities of users and devices at communication session endpoints will disable unauthorized access and repudiation. The restriction of each user's privileges to the minimum necessary for operation and maintenance is essential for ICS security.

Prerequisites and limitations:

Open logical access may be necessary, i.e. for functional-safety-oriented control-room operation. This exception should be controlled by restricting physical access to the control room.

Implementation guidance:

8.3.1.1 Factory default credentials should be removed.

8.3.1.2 Only operationally required accounts with operationally required privileges should be assigned to users and devices on a least privilege basis and according to their respective role.

NOTE 1 Default accounts or legacy accreditations have been historically one of the biggest security weaknesses and are assumed removed at installation time by system integrity action, refer to 8.2.3.1.

NOTE 2 Least privilege is a security principle granting each system entity the minimum system resources and authorizations required to do its work.

NOTE 3 Role-based access control is a well-established scheme for managing and rationalizing access rights for larger groups of users/devices with varying access requirements, and may include presence at physical location and associated time-slots.

NOTE 4 Separation of users into different mutually controlling roles reduces likelihood of insider attacks.

8.3.1.3 Access control accounts and privileges should be updated when staff leaves or changes roles.

NOTE Changes should be implanted swiftly after occurring, i.e. after terminations, changes in assignments and device configurations.

8.3.1.4 Authentication should use strong credentials.

NOTE Length and characteristic of passwords should be controlled to be strong enough to prevent bypassing, for example, by guessing or brute force cracking. If considered weak, additional factors should be added, i.e. dongles, biometrics, physical location at authenticating console.

8.3.1.5 Privileges should be established for files, applications, O/S tools, services, devices and partitions, on the finest granular level reasonably feasible.

NOTE 1 Some O/S utilities allow significant modifications of the state and configuration of the host and the whole automation system. Most users of the ICS, such as operators, may not need to access part or all of these utilities.

NOTE 2 Communication channels from/to the outside of the partition and between partitions should be associated to access rights for users/devices to those partitions.

NOTE 3 The privilege to install executables, i.e. applications, should be strictly controlled.

8.3.1.6 Communications privileges should be established separately for to and from (source and destination) basis for devices, hosts, and media.

NOTE 1 Particular attention has to be given to IP address assignment and management, i.e., address translation, partition versus subnet masks, directory service and location of related servers, domain name services (DNS), prevent network address translation (NAT) to be used on the ICN.

NOTE 2 Broad assignments such as drive mapping/mounting or "directed" broadcasts to/from external networks should not be allowed.

8.3.1.7 Privileges to change configuration settings in operating systems and hardware should be strictly controlled.

8.3.1.8 Privileges to change security relevant configuration settings on switches, routers, IDSs, SGWs, etc. strongly impact correct function of the ICS and should receive strong access control protection.

8.3.1.9 Specific periodic review procedures of access control privileges should be established to assure that privileges and level assigned to each user/device are current and conforming to actual use, justification and current requirements.

8.3.2 Additional confidentiality measures should be implemented in case of weak access control measures and/or higher confidentiality requirements.

Rationale:

Protecting access to devices and media containing confidential data may not be sufficient for higher data confidentiality requirements, for example, in the presence of untrusted cabling or for user credentials. In this case encryption may be required.

Implementation guidance:

8.3.2.1 In SEDs, sensitive manufacturing data should be to be protected apart from program data.

8.3.2.2 Encryption methods should be changed and reviewed to assure withstanding reasonable brute force attack for foreseeable time periods.

NOTE 1 Strong encryption implies periodic key changes and key management, as well as periodic re-keying and secure media/data disposal methods.

NOTE 2 The time between those chances must be balanced between security requirements and disturbance of the communication channel between both sides.

8.3.3 Additional non-repudiation measures should be implemented in case of higher non-repudiation requirements.

Rationale:

Ensuring accountability through non-repudiation is one of the most important measures against insider attacks.

NOTE Cryptographic measures may be suitable.

8.3.4 Authentication privileges, key exchange and access control mechanisms should be installed, initialized and managed on designated equipment according to assigned privileges.

Rationale:

Access control requires authentication.

Prerequisites and limitations:

Organizational emergency override capability to bypass failed authentication should be defined, for example, for possible technical failures of the authentication/access control subsystem or absence of the operator.

Implementation guidance:

8.3.4.1 Effective administration of privileges should be assured using tools, and if possible, automated means such as authentication servers and key centres.

NOTE Authentication servers and key centres contain highly sensitive data and should be located inside the plant, controlled by ICN administration, and protected logically and physically.

8.3.4.2 System action in the event of authentication failure should be defined.

NOTE 1 Standards action may be defined as, for example, unlimited retry, unlimited retries with progressive delay, or lock-out after a limited number of retries, and possible generation and escalation of alarms.

NOTE 2 An escrow procedure may be created which makes sure that a situation of uncontrolled user access or repudiation of actions cannot occur.

8.3.5 Authentication privileges, key exchange and access control mechanisms should be monitored and logged.

Rationale:

Logs associate users and devices with actions and enables attribution of causes and responsibility.

Prerequisites and limitations:

Certain privacy legislations may require reduction or anonymizing of log data.

Implementation guidance:

8.3.5.1 The user, or at least the user that established the session, should be logged with time and all security relevant actions taken from that console.

NOTE Refer to ISO/IEC monitoring system access and use in ISO/IEC 27002.

8.4 Physical access management

This ensures only authorized physical access to ICS resources by location and according to assigned privileges, including authorized equipment and tools, media or information in general.

8.4.1 Hosts, devices and media should be protected against illicit access, removal, destruction and theft according to protection requirements.

Rationale:

In complement of logical protection, ICS should provide physical protection, through arming and locking of hosts, devices and media against illicit access, removal, destruction and theft.

NOTE Equipment to be secured physically includes

- rooms, cabinets, cases of switches, SGWs, PC enclosures;
- mobile equipment and media such as PCs and lap-tops;
- USB ports, floppy disk drives;
- self-contained industrial control devices;
- cabling.

8.4.2 Identities, keys and other user/device credentials and rights/privileges should be managed.

Rationale:

The assignment of user access privileges for operation and maintenance of ICS equipment is essential for ICS security.

Prerequisites and limitations:

Reliability and trustworthiness of personnel should be established by personnel management.

Implementation guidance:

8.4.2.1 Access privileges should be associated to access through gates from/to the outside of the partition and possibly within partitions.

8.4.3 Physical access to equipment rooms, cabinets and cases should be monitored, logged and alarmed.

Rationale:

Verification of the identities of users accessing closed physical partitions will reduce unauthorized access and repudiation. Logs associate the user, or at least the user who operated the access control mechanism, with time and assures attribution of responsibility.

Prerequisites and limitations:

TV monitoring may be excluded by union agreements or local law.

Implementation guidance:

8.4.3.1 Critical PAGs and/or partitions should to be staffed or TV-monitored to detect violations and violators.

8.4.3.2 Awareness training on peer personnel watch should be part of efficient physical access management.

8.4.3.3 Critical PAGs and/or partitions should to be staffed or TV-monitored to maintain awareness.

8.4.3.4 Response to physical access control violations should be managed and coordinated with humans resources.

8.5 Partition management

Structuring of the ICS into separated logical and/or physical partitions, protected by SGW and/or PAG, efficiently reduces the attack surface by adding another parameter to the assignable privilege parameters.

NOTE 1 Different logical partitions may be interconnected, for example, by a backbone, on the same level or into a hierarchical structure.

NOTE 2 For the interconnections between the ICN and any EN, refer to 8.6.

8.5.1 PAGs and SGWs should be implemented to protected logical and physical partition borders according to access control rules, protection requirements and topology.

Rationale:

Usually it is more economical to secure equipment, HMI and cabling by grouping, i.e., by a separate zone, room, cabinet or armature, and a single entry point rather than individually by multiple access points.

Implementation guidance:

8.5.1.1 Each partition should be protected by a SGW at a single entry point to/from the common backbone or subordinated partition.

NOTE SGW function and any related supporting functions should be implemented on dedicated hosts or appliances.

8.5.1.2 The SGWs should allow communication to its protected zone only from stations in trusted zones or trusted devices from the backbone.

NOTE All unnecessary communications should be blocked, i.e., those that have no explicit business need and/or for which no one is explicitly responsible.

8.5.1.3 SGW access control to the partition may additionally be controlled by cryptographically protected protocols or PAG.

NOTE Equipment, facilities, functions and duties should be grouped electrically, logically and physically according to functionality and protection requirements.

8.5.1.4 Each SGW should log security relevant actions such as attempts to access its protected partition.

8.5.2 Logical and/or physical activity within partitions should be constantly monitored to detect or capture irregular or dubious activity (i.e., intrusion), create relevant logs and trigger alarms.

Rationale:

PAGs and SGWs are single points of potential intrusion through the partition border and thus suitable and preferred indicators of illicit activity. This border control should be complemented by internal measures such as IDS, in particular for insider threats.

Implementation guidance:

8.5.2.1 IDS should be implemented to detect illicit insider activity and successful intrusion.

NOTE 1 The IDS sensor should be non-addressable but listen-only to eliminate the likelihood of it being attacked.

NOTE 2 The capabilities of host-based IDS, network-based IDSs, and file system integrity checkers are complementary.

NOTE 3 A host-based intrusion detection system should include alerts of users on a host.

8.5.2.2 Indicators, for example, in the control system, HMI and/or alarm management subsystem should alert operators to problems with the change in dataflow caused by a reaction to a detected attack.

8.5.2.3 Deflection measures, i.e., honey-pots and decoys, provide additional detection capability after intrusion.

8.5.2.4 Monitoring/support personnel should be notified in advance of any rule change that may trigger a SGW alarm.

8.5.3 PAGs and SGWs should be securely administered.

Rationale:

SGWs need to be securely administered to ensure that access rules and their enforcement withstand evolving threats.

Implementation guidance:

8.5.3.1 Management should include hosts, network equipment rooms, cabinets, cases, cabling.

8.5.3.2 Security management traffic should receive particular attention.

NOTE Security management communication channels should be separate from production traffic channels.

8.5.3.3 Particular attention has to be paid to protection of security management traffic to/from external networks, for example, with external security service providers or remote partitions.

8.6 External access management

All communications between the ICN and networks and devices external to the ICN are considered untrusted unless secured, as the organizational EN, and even more a public EN have a significantly larger, more diverse and less trusted user population than the ICN.

8.6.1 External connectivity should be approved and implemented only if necessary for the operation, management, and maintenance of the ICS.

Rationale:

Intentional or incidental import of malicious files into the system is a significant threat.

Implementation guidance:

8.6.1.1 Procedures should be established and enforced to protect against importing unauthorized or infected files from untrusted sources such as networks and portable storage media.

NOTE Corresponding prescriptions in the security policy may be augmented by technical means.

8.6.1.2 ICS management should have full control over all data imported into the ICN as well as the timing of this import.

8.6.1.3 Portable devices brought physically into the plant such as lap-tops and data-media should be considered as external devices.

8.6.1.4 For critical files, i.e., executables, imported physically or electronically, ICS management should establish and enforce procedures to verify that all files are required, suitable for use, free of malware, have not been tampered with on transit and are imported to the correct destination.

NOTE 1 Physical import means import of portable storage media, lap-tops and other portable electronic devices.

NOTE 2 Physical imports should be handled in concert with hardening procedures by restriction of their possible destinations, i.e. interfaces and access ports.

8.6.1.5 Approval procedures for temporary *ad hoc* connections should be available, for example, for update and maintenance operations by vendors.

8.6.1.6 For continuous on-line sessions, session keys should be changed frequently, for example, by renewed log-in.

NOTE Security requirements should be balanced with the disturbance of the communication channel.

8.6.1.7 All in-plant and out-of-plant communications possibilities should be monitored for illicit use.

NOTE Communications possibilities to be monitored include POTS (voice-grade traditional telephone service), radiofrequency, cell-phone, wireless, etc.

8.6.2 External communications connectivity should be protected by ECG according to protection requirements.

Rationale:

All communication between the ICS hosts, devices and external networks or devices should be protected against threats from the organizational EN and the virtually unlimited threats from public ENs.

Prerequisites and limitations:

Wholesale access, i.e., broadcasts, file mounting, across ECG is assumed to be denied by access control policy.

Implementation guidance:

8.6.2.1 Appropriate mechanisms should only be used to assure, i.e., source integrity, data integrity and, if required, confidentiality.

NOTE Proprietary security mechanisms may not function correctly through the ECG and may require special handling.

8.6.2.2 Proxy services should be implemented if required for adequate protection, including authentication.

This prevents threats from an EN, for example, direct observation of ICN, the traffic and protocol characteristics of hosts on the ICN. It also allows for screening of the incoming and outgoing communication content on the application level.

8.6.3 Access to/from external users/devices should be managed and logged.

Rationale:

This requirement serves to secure communications with the remote access link, to deter attacks from insiders using the remote client, and to track respectively evidence attacks and intrusion.

Implementation guidance:

8.6.3.1 When no remote access session is required, external users/device communications should be disabled for the corresponding timeframes.

NOTE Electrically disconnecting the users/device or communications line should be more secure than logically blocking remote access user accounts at the ESG or proxy.

8.6.3.2 For critical communications, logging of external access activity should allow session replay in full detail.

8.6.4 Security of remote clients should be certified, authorized and managed.

Rationale:

To establish and maintain trust, remote clients require appropriate technical mechanisms and their configurations, and are subject to ICS security policy.

NOTE Included are remote control centre, remote hosts, remote workstations, remote devices.

Prerequisites and limitations:

If managed by a different organization than the ICS this organization may have different IT security policies. In this case detailed contractual agreements between the ICS organization and the remote client organization will be necessary.

Implementation guidance:

8.6.4.1 ICS policy should be enforced to the remote client for the entire extent and timeframe of use with and connection to the ICN.

8.6.4.2 Assigned services and ports should be preconfigured, for example, using caller identification or fixed dial-back for telephone networks; or secure channels.

8.6.4.3 ICS management should periodically audit the adherence of the remote client to ICS policy or contractual agreements.

8.6.5 External communications access rules should be enforced and monitored by SGWs.

Rationale:

Technical means should be used to ensure that ICS staff is aware of all ongoing remote access sessions and can control the timing of remote access sessions.

Implementation guidance:

8.6.5.1 SGWs should be centrally monitored.

8.6.5.2 Response to access control violations should be defined, documented, and acted upon immediately after occurrence according to contingency plan.

8.6.5.3 Response to availability problems should be defined, documented, and executed upon immediately after occurrence according to contingency plan.

Refer to reporting information security events and weaknesses in ISO/IEC 27002.

8.6.6 Availability risk of critical external communications channels may be mitigated.

Rationale:

Availability may be an important aspect for ICS operation and maintenance.

Prerequisites and limitations:

Break-down of a communications channel during denial of service attack cannot be prevented, as security mechanisms applied to ICN hosts and/or communications devices have no effect on external communications availability.

Availability of any individual EN communications channel is not under the control of ICS management and therefore cannot be assured with any reasonable degree of certainty.

Implementation guidance:

8.6.6.1 Communication rate bandwidth should be assigned according to importance for operation and maintenance.

NOTE Available bandwidth can be allocated to several users, rate-limited and prioritized.

8.6.6.2 Redundancy and/or diversity techniques should be used to enhance availability.

NOTE 1 Diversity techniques include use of separate providers, public network supplemented by POTS or wireless.

NOTE 2 Diverse or simple redundancy increase exposure to attack (see 8.1.1.1).

Annex A

Projected new edition of IEC 62443

Under the general title, *Security for industrial process measurement and control – Network and system security*, a projected new edition of IEC 62443 will consist of the following parts:

Part 1: Framework and threat-risk analysis

Part 2: Security assurance: principles, policy and practice

Part 3: Sets of security requirements for typical security scenarios

The projected edition of IEC 62443 is seeking the status of a basic security publication similar to basic safety publications according to IEC Guide 104.

Introduction

The increasing degree of public networking of formerly isolated automation systems increases the exposure of such systems to attack. Standard IT security mechanisms have protection goals, and strategies may not be appropriate for automation systems, for example, when timely response may be critical to the security and safety of plant personnel, the environment and the corporation. This International Standard will address the specific aspects of securing access to and within industrial systems, particularly where more widely available IT-based security techniques prove insufficient or inappropriate.

Special emphasis is given to addressing the security lifecycle in a holistice manner to move from add-on of security system components to integrating required security properties into the products and systems as integral part of their functionality and life-cycle.

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).

Scope

This International Standard will establish requirements for securing access to industrial process measurement and control networks and devices on those networks during the whole life cycle of an ICS.

This international standard will provide requirements and guidance on security objectives to:

- automation system designers;
- manufacturers (vendors) of devices, subsystems, and systems;
- integrators of subsystems and systems;
- automation system owners/operators (responsible for plant operation);

The International Standard will consider the following concerns:

- graceful migration/evolution for existing systems, measures during development of new systems and components;
- technologies and products to meet security objectives, including COTS;
- fail-over modes that are process-safe, including response to denial of service (for example, autonomous operation);
- reliability/availability;
- scalability (from complex factories down to small, low-cost, low-risk systems);
- separation of security, safety and functionality requirements as much as appropriate;

- consideration of security aspects during development of automation systems and components.

NOTE Plants and systems may contain safety critical components and devices, specifically devices developed based on IEC 61508 and according to the SILs therein. The safety critical components and devices may have security objectives determined through separate analysis. These security objectives may be met using the guidance provided in this International Standard, but this International Standard does not guarantee that its specifications are all appropriate or sufficient for the security of such safety devices. It is not the aim of this International Standard to address the issues of home security, citizen protection, protection against war attacks or natural disasters.

Part 1 of IEC 62443 will allow the user to evaluate his/her security situation i.e. in terms of applicable threats and exposure and prepares for security risk management for the entire life cycle of his/her systems. It includes

- vocabulary, terms definitions, target audiences, application area, stakeholders, roles;
- communalities and differences of industrial control systems compared to common IT applications;
- event (attack) scenarios;
- life cycle;
- expected results of a threat-risk analysis;
- examples for:
  - security objectives;
  - vulnerability analysis;
  - risk assessment.

Part 2 of IEC 62443 will enable the users of the standard to define and implement their security policy and the resulting requirements down to the desired practical aspects and level of detail and all life cycle phases. It will deal with

- assurance principles, classification, assessment;
- principles: development of devices, design criteria, properties of devices;
- consideration of legacy devices, COTS and devices under development;
- consideration of security aspects during development of components (not only security components) of industrial control systems (sensors/actuators/PLC/network/server/HMI).

Part 3 of IEC 62443 will give the user samples of good practice security solutions for typical scenarios as help for his/her specific implementation:

- sample scenarios and security measures;
- sample security policies, process descriptions and procedures.

Bibliography

[1] ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*

[2] ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*

[3] ISO/IEC TR 13335-5:2001, *Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security*

[4] ISO/IEC 15288:2002, *Systems engineering — System life cycle processes*

[5] ISO/IEC TR 15443-1:2005*, Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework*

[6] ISO/IEC 15446:2004, *Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets*

[7] ISO/IEC 21827:2002, *Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)*

[8] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

[9] IEC 61508:1998 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[10] NIST SP 800-82, *"Guide to Supervisory Control and Data Acquisition (SCADA) and Other Industrial Control System Security"*, Initial Public Draft, September 2006

[11] NIST SP 800-53, *"Recommended Security Controls for Federal Information Systems"*, Second Public Draft, July 2006

[12] *"Technology Assessment -- Cybersecurity For Critical Infrastructure Protection"*, United States General Accounting Office, May 2004

[13] *"Cyber Security Procurement Language for Control Systems"*, Draft, November 2006, Idaho National Laboratory, Idaho Falls, ID 83415, USA

[14] *"Systems Assurance – Delivering Mission Success in the Face of Developing Threats"*, Systems Assurance Committee, NDIA, USA

[15] *"A study of the applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the needs of safety critical systems"*, EWICS (European Workshop on Industrial Computer Systems) Technical Committee No. 7: Reliability, Safety and Security; Roadmap D31. http://www.ewics.org/docs/roadmap-project

[16] "Good Automated Manufacturing Practice (GAMP): Guide for Validation of Automated Systems in Pharmaceutical Manufacture", ISPE, 3109 W. Dr. Martin Luther King Jr. Blvd., Suite 250, Tampa, FL 33607, USA

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
P.O. Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch