# IEC/TR 62443-3-1

Edition 1.0 2009-07

# TECHNICAL REPORT

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

colour inside

## Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

IEC/TR 6244-3-1:2009(E)

**THIS PUBLICATION IS COPYRIGHT PROTECTED**

**Copyright © 2009 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.
If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.
Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

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 It also gives information on projects, withdrawn and replaced publications.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

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

# IEC/TR 62443-3-1

Edition 1.0 2009-07

# TECHNICAL REPORT

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

colour inside

## Industrial communication networks – Network and system security – Part 3 1: Security technologies for industrial automation and control systems

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XD

ICS 25.040.40; 33.040.040; 35.040

ISBN 978-2-88910-711-7

® Registered trademark of the International Electrotechnical Commission

# CONTENTS



IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1:2009

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

## Part 3-1: Security technologies for industrial automation and control systems

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

## 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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62443-3-1, which is a technical report, has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This technical report is closely related to ANSI/ISA-TR99.03.01-2007.

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

| Enquiry draft | Report on voting |
|---|---|
| 65/424/DTR | 65/431A/RVC |

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with ISO/IEC Directives, Part 2.

A list of all parts of IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under http://webstore.iec.ch in the data related to the specific publication. At this date, the publication will be:

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

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

NOTE The revision of this technical report will be synchronized with the other parts of the IEC 62443 series.

**IMPORTANT – The "colour inside" logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.**

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

# INTRODUCTION

The need for protecting Industrial Automation and Control System (IACS) computer environments from malicious cyberintrusions has grown significantly over the last decade. The combination of the increased use of open systems, platforms, and protocols in the IACS environment, along with an increase in joint ventures, alliance partners and outsourcing, has lead to increased threats and a higher probability of cyberattacks. As these threats and vulnerabilities increase, the risk of a cyberattack on an industrial communication network correspondingly increases, as well as the need for protection of computer and networked-based information sharing and analysis centres. Additionally, the growth in intelligent equipment and embedded systems; increased connectivity to computer and networked equipment and software; and enhanced external connectivity coupled with rapidly increasing incidents of network intrusion, more intelligent hackers, and malicious yet easily accessible software, all add to the risk as well.

There are numerous electronic security technologies and cyberintrusion countermeasures potentially available to the IACS environment. This technical report addresses several categories of cybersecurity technologies and countermeasure techniques and discusses specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for their deployment, and their known strengths and weaknesses. Additionally, guidance is provided for using the various categories of security technologies and countermeasure techniques for mitigation of the above-mentioned increased risks.

This technical report does not make recommendations of one cybersecurity technology or mitigation method over others, but provides suggestions and guidance for using the technologies and methods, as well as information to consider when developing a site or corporate cybersecurity policy, program and procedures for the IACS environment.

The responsible standards development working group intends to update this technical report periodically to reflect new information, cybersecurity technologies, countermeasures, and cyberrisk mitigation methods. The committee cautions the reader that following the recommended guidance in this report will not necessarily ensure that optimized cybersecurity is attained for the reader's industrial automation or control systems environment. It will, however, help to identify and address vulnerabilities, and to reduce the risk of undesired cyberintrusions that could compromise confidential information or, even worse, cause human and environmental harm, as well as disruption or failure of the industrial network or control systems and the industry and infrastructure critical assets they monitor and regulate.

This technical report provides an evaluation and assessment of many current types of electronic-based cybersecurity technologies, mitigation methods and tools that may apply to protecting the IACS environment from detrimental cyberintrusions and attacks. For the various technologies, methods and tools introduced in this report, a discussion of their development, implementation, operations, maintenance, engineering and other user services is provided. The report also provides guidance to manufacturers, vendors, and security practitioners at end-user companies, facilities, and industries on the technological options and countermeasures for securing automated IACSs (and their associated industrial networks) against electronic (cyber) attack.

Following the recommended guidance given in this technical report will not necessarily ensure that optimized cybersecurity is attained for IACSs. It will, however, help to identify and address vulnerabilities, and to reduce the risk of undesired intrusions that could compromise confidential information or cause disruption or failure of control systems and the critical infrastructure assets they automate and control. Of more concern, use of the recommendations may aid in reducing the risk of any human or environmental harm that may result after the cyber compromise of an automated control system or its associated industrial network.

The cybersecurity guidance presented in this document is general in nature, and should be applied to each control system or network as appropriate by personnel knowledgeable in those specific industrial automation or control systems to which it is being applied. The guidance identifies those activities and actions that are typically important to provide cybersecure control

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

systems, but whose application is not always compatible with effective operation or maintenance of a system's functions. The guidance includes suggestions and recommendations on appropriate cybersecurity applications to specific control systems. However, selection and deployment of particular cybersecurity activities and practices for a given control system and its related industrial network is the responsibility of the system's owner.

It is intended that this guidance will mature and be modified over time, as experience is gained with control system vulnerabilities, as specific cybersecurity implementations mature, and as new control-based cybersecurity technologies become available. As such, while the general format of this guidance is expected to remain relatively stable, the specifics of its application and solutions are expected to evolve.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

# INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

## Part 3-1: Security technologies for industrial automation and control systems

## 1 Scope

This part of IEC 62443 provides a current assessment of various cybersecurity tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary recommendations and guidance for using these cybersecurity technology products and/or countermeasures.

The concept of IACS cybersecurity as applied in this technical report is in the broadest possible sense, encompassing all types of components, plants, facilities, and systems in all industries and critical infrastructures. IACSs include, but are not limited to:

- Hardware (e.g., data historian servers) and software systems (e.g., operating platforms, configurations, applications) such as Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, networked electronic sensing systems, and monitoring, diagnostic, and assessment systems. Inclusive in this hardware and software domain is the essential industrial network and any connected or related information technology (IT) devices and links critical to the successful operation to the control system at large. As such, this domain also includes, but is not limited to: firewalls, servers, routers, switches, gateways, fieldbus systems, intrusion detection systems, intelligent electronic/end devices, remote terminal units (RTUs), and both wired and wireless remote modems.
- Associated internal, human, network, or machine interfaces used to provide control, data logging, diagnostics, safety, monitoring, maintenance, quality assurance, regulatory compliance, auditing, and other types of operational functionality for either continuous, batch, discrete, and combined processes.

Similarly, the concept of cybersecurity technologies and countermeasures is also broadly applied in this technical report and includes, but is not limited to, the following technologies:

- authentication and authorization;
- filtering, blocking, and access control;
- encryption;
- data validation;
- auditing;
- measurement;
- monitoring and detection tools;
- operating systems.

In addition, a non-cyber technology —physical security control— is an essential requirement for some aspects of cybersecurity and is discussed in this technical report.

The purpose of this technical report is to categorize and define cybersecurity technologies, countermeasures, and tools currently available to provide a common basis for later technical

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

reports and standards to be produced by the ISA99 committee. Each technology in this technical report is discussed in terms of:

- security vulnerabilities addressed by the technology, tool, and/or countermeasure;
- typical deployment;
- known issues and weaknesses;
- assessment of use in the IACS environment;
- future directions;
- recommendations and guidance;
- information sources and reference material.

The intent of this technical report is to document the known state of the art of cybersecurity technologies, tools, and countermeasures applicable to the IACS environment, clearly define which technologies can reasonably be deployed today, and define areas where more research may be needed.

## 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.

<none>

## 3 Terms, definitions and acronyms

### 3.1 Terms and definitions

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

**3.1.1**
**access authority**
entity responsible for monitoring and granting access privileges to IACSs and their associated industrial networks for other authorized entities [3][1]

**3.1.2**
**access control**
a) protection of system resources against unauthorized access

b) process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy [3]

**3.1.3**
**accountability**
property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions [3]

**3.1.4**
**application layer protocol**
layer 7 protocol specific to executing network applications such as email and file transfer [2]

[1] Numbers in square brackets refer to the Bibliography.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

NOTE Many modern industrial control systems include fieldbus networks, which do not normally include seven distinct layers, but have an application layer.

**3.1.5**
**asymmetric key algorithm**
public key cryptographic algorithm

NOTE By asymmetric, the key for encoding the digital data to be transmitted is entirely different from the code for decrypting the data at the receiving end. This is in contrast to symmetric key encryption, whereby the same key is used to encrypt and decrypt the data. Asymmetric is logistically more secure because it avoids transfer of the key between transmitter and receiver, whereby it could be intercepted. It is important to note that cryptographic methods to protect the confidential data are more critical for IT networks than for control networks. For IACSs, confidentiality is most critical for the authenticating and authorization stages during access control into a given IACS. Usually cryptography adds undesired latency to the IACS network, which is very undesirable for open and closed loop systems that must receive, manipulate, and send control data at a rate commensurate to an asset's process dynamics. Consequently, availability and integrity are usually higher IACS cyber security objectives than is confidentiality. [3]

**3.1.6**
**authentication**
security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information [4]

**3.1.7**
**authorization**
right or a permission that is granted to a system entity to access a system resource [3]

**3.1.8**
**availability**
probability that an asset, under the combined influence of its reliability, maintainability and security will be able to fulfil its required function over a stated period of time or at a given point in time

**3.1.9**
**bandwidth**
capacity of a communication channel to pass data through the channel in a given amount of time

NOTE 1 Bandwidth, in the sense of channel capacity, usually is expressed in bits per second.

NOTE 2 Control and SCADA data are usually of smaller, yet consistent, bit sizes than IT networks, which traditionally carry higher levels. Nonetheless, the move to fieldbus systems requires higher band widths due to their inherent nature of requiring less wiring and performing control algorithms without the use of a master station or PLC. [3]

**3.1.10**
**certificate**
public key certificate [3]

**3.1.11**
**certification authority**
entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates, and exacting compliance to a PKI policy [3]

**3.1.12**
**ciphertext**
data that have been transformed by encryption so that the semantic information content (i.e., meaning) is no longer intelligible or directly available

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

**3.1.13**
**cleartext**
data in which the semantic information content (i.e., meaning) is intelligible or is directly available [3]

**3.1.14**
**client**
device or application receiving or requesting services or information from a server application [1]

**3.1.15**
**confidentiality**
assurance that information is not disclosed to unauthorized individuals, processes or devices [4]

**3.1.16**
**cryptographic key**
input parameter that varies the transformation performed by a cryptographic algorithm [3]

NOTE This is usually shortened to “key”.

**3.1.17**
**cyberattack**
successful exploitation of the software, hardware or firmware vulnerabilities of IACS components and/or the IT network components connected to the industrial network

**3.1.18**
**data-link layer protocol**
layer 2 protocol for point-to-point communications of data, conducting error checking, performing physical addressing and conducting media access control [2]

NOTE These protocols exist in most IT enterprise systems connected to control LANs and in some cases exist in the protocols of industrial networks.

**3.1.19**
**decryption**
process of changing ciphertext into plaintext using a cryptographic algorithm and key (see 3.1.24 “encryption”) [3]

**3.1.20**
**defence in depth**
security architecture based on the idea that any one point of protection may, and probably will, be defeated

NOTE Defence in depth implies layers of security and detection, even on single systems, and provides the following features:

- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be protected by capabilities in other layers;
- system security becomes a set of layers within the overall network security.

**3.1.21**
**denial of service**
**DoS**
prevention or interruption of authorized access to a system resource or the delaying of system operations and functions [3]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

**3.1.22**
**digital signature**
result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation [1]

**3.1.23**
**distribution**
key distribution [3]

**3.1.24**
**encryption**
cryptographic transformation of plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used (see 3.1.19 "decryption") [3]

NOTE If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

**3.1.25**
**integrity**
quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data [4]

NOTE In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

**3.1.26**
**interception**
capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission and other communication attributes

**3.1.27**
**interface**
logical entry or exit point that provides access to the module for logical information flows

**3.1.28**
**key**
cryptographic key

**3.1.29**
**key distribution**
transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key [3]

**3.1.30**
**key pair**
public key and its corresponding private key used with a public key algorithm [3]

**3.1.31**
**local area network**
**LAN**
communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 km) [5]

**3.1.32**
**latency**
time interval between when a message is sent by one device and received by a second device

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

NOTE Latency, along with jitter, are two key parameters that define the performance of a control system. Increased latency for a control loop can be detrimental since the dynamics of the asset under control dictates the amount of latency to keep the control process safe and productive.

**3.1.33**
**man-in-the-middle**
active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association

NOTE This is also defined as snooping and can be effectively misleading and destructive in an IACS cyber attack since a control room operator's screen may be indicating safe and normal routine operation, while havoc is conducted on the automated processes and assets in the field. [3]

**3.1.34**
**network layer protocol**
layer 3 protocol for routing of messages through a complex network [2]

NOTE Most modern industrial fieldbus protocols and SCADA protocols usually contain a network layer.

**3.1.35**
**non-repudiation**
security service that provides protection against false denial of involvement in a communication [3]

**3.1.36**
**password**
string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization [1]

**3.1.37**
**personal identification number**
**PIN**
alphanumeric code or password used to authenticate an identity [1]

**3.1.38**
**physical layer protocol**
layer 1 protocol for transmitting raw physical (e.g. electro-magnetic) signals over a communications channel

NOTE Layer 1 deals with transmission physics such as cabling, modulation, and transmission rates. [2]

**3.1.39**
**plaintext**
unencoded data that is input to and transformed by an encryption process or that is output by a decryption process [3]

**3.1.40**
**point-to-point protocol**
**PPP**
protocol defined in RFC 1661, the Internet standard for transmitting network layer datagrams (e.g., Internet Protocol (IP) packets) over serial point-to-point links, which is occasionally deployed in certain types of SCADA networks

**3.1.41**
**protection profile**
implementation-independent set of security requirements for a category of targets of evaluation that meet specific consumer needs [1]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

**3.1.42**
**pseudorandom number generator**
**PRNG**
algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed

NOTE The output of a PRNG should appear to be uniform random, i.e., the output is statistically indistinguishable from uniform random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. [3]

**3.1.43**
**public key**
cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public [1]

**3.1.44**
**public key certificate**
dataset that uniquely identifies an entity, contains the entity's public key and is digitally signed by a trusted party, thereby binding the public key to the entity [1]

**3.1.45**
**public key (asymmetric) cryptographic algorithm**
cryptographic algorithm that uses two related keys, a public key and a private key, such that deriving the private key from the public key is computationally infeasible

**3.1.46**
**public key infrastructure**
**PKI**
framework that is established to issue, maintain and revoke public key certificates [3]

**3.1.47**
**repudiation**
denial by one of the entities involved in a communication of having participated in all or part of the communication [3]

**3.1.48**
**risk**
expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [3]

**3.1.49**
**secret key**
cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public [1]

**3.1.50**
**secret key (symmetric) cryptographic algorithm**
cryptographic algorithm that uses a single secret key for both encryption and decryption [1]

**3.1.51**
**security domain**
system or subsystem of a control LAN or enterprise LAN that is under the authority of a single trusted authority

NOTE Security domains may be organized (e.g. hierarchically) to form larger domains. [3]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

**3.1.52**
**security services**
mechanisms used to provide confidentiality, data integrity, authentication or no repudiation of information [3]

**3.1.53**
**server**
device or application that provides information or services to client applications and devices [3]

**3.1.54**
**sniffing**
interception

**3.1.55**
**spoof**
pretending to be an authorized user and performing an unauthorized action [3]

**3.1.56**
**symmetric key**
single cryptographic key that is used with a secret (symmetric) key algorithm

NOTE A system whereby the encrypting key from plain text to cipher text is identical to the key to convert the cyber text back to plain text. [3]

**3.1.57**
**symmetric key algorithm**
secret key cryptographic algorithm [3]

**3.1.58**
**system software**
special software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs and data [1]

**3.1.59**
**threat**
potentially damaging action (intended or unintended) or capability (internal or external) to adversely impact through a vulnerability [6]

**3.1.60**
**throughput**
maximum continuous traffic rate that an IT or IACS device can handle without dropping a single packet [2]

**3.1.61**
**vulnerability**
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy [3]

**3.1.62**
**wide area network**
**WAN**
communications network designed to connect computers over a large distance, such as across a country or the world [1]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

### 3.2 Acronyms

All trade names and trademarks used in this document are listed in Annex A.

| | |
|---|---|
| 3DES | Triple Digital Encryption Standard |
| AES | Advanced Encryption Standard |
| AGA | American Gas Association |
| ASM | Automated Software Management |
| CERT | Computer Emergency Response Team |
| CHAP | Challenge Handshake Authentication Protocol |
| CIP® | Common Industrial Protocol (formerly Control and Information Protocol) |
| CMVP | Cryptographic Module Validation Program |
| COTS | Commercial Off The Shelf |
| CPU | Central Processing Unit |
| CS | Control System |
| DAC | Discretionary Access Control |
| DC | Domain Controller |
| DCS | Distributed Control Systems |
| DMZ | Demilitarized Zone |
| DoS | Denial-of-Service |
| DPA | Differential Power Analysis |
| EC | Elliptic Curve |
| ECC | Elliptic Curve Cryptosystem |
| FAN | Field Area Network |
| FAQ | Frequently Asked Questions |
| FAT | Forensics and Analysis Tool |
| FIPS | Federal Information Processing Standards |
| FTP | File Transfer Protocol |
| GPS | Global Positioning System |
| HCM | Host Configuration Management |
| HIDS | Host Intrusion Detection System |
| HMI | Human Machine Interface |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| IACS | Industrial Automation and Control System |
| IAONA | Industrial Automation Open Networking Association |
| IATF | Information Assurance Technical Framework |
| ID | Identification |
| IDS | Intrusion Detection System |
| IED | Intelligent Electronic Devices |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| IT | Information Technology |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LSS | Location Signature Sensor |

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

| | |
|---|---|
| MAC | Media Access Control |
| MIT | Massachusetts Institute of Technology |
| NAT | Network Address Translation |
| NFA | Network Forensics and Analysis |
| NIDS | Network Intrusion Detection System |
| NIST | U.S. National Institute of Standards and Technology |
| NSA | U.S. National Security Administration |
| OLE® | Object Linking and Embedding |
| OPC® | OLE for Process Control |
| OS | Operating System |
| PC | Personal Computer |
| PCN | Process Control Network |
| PDA | Personal Digital Assistant |
| PGP® | Pretty Good Privacy® |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PLC | Programmable Logic Controller |
| PPP | Point-to-Point Protocol |
| PRNG | Pseudorandom Number Generator |
| RBAC | Role-Based Access Control |
| RFC | Request For Comment |
| RSA® | Rivest, Shamir and Adleman |
| RTOS | Real-time Operating System |
| RTU | Remote Terminal Unit |
| SAM | Security Accounts Manager |
| SCADA | Supervisory Control and Data Acquisition |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| Sysdiff | System Difference Packages |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |
| USB | Universal Serial Bus |
| VDS | Virus Detection System |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| Wi-Fi | Wireless Fidelity |

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

## 4 Overview

Many industries and critical infrastructures have reported an increase in the number of unauthorized attempts to access electronic information, or even more ominous, hack into IACSs that monitor and regulate assets crucial for a nation (e.g. energy pipelines, transportation systems, water systems, the power grid). Over the last several years, the number of joint ventures, alliance partners and outsourced services in the industrial sector has

increased dramatically. During that same period, IACSs have evolved from isolated networks based on proprietary technologies and protocols to standards-based networks connected to the rest of the enterprise—including the IT business enterprise usually connected to the Internet and to other enterprises such as partners and corporate WANs.

Consequently, it is now very challenging to know *who* is authorized to have access to electronic IACSs information, *when* they are to have access to the information and *what* data they should be able to access. Partners in one business venture may also be competitors in another business. However, because IACS equipment is directly connected to a process, loss of trade secrets or interruptions in the flow of information are not the only potential consequences of a security breach and certainly not the ones with the greatest impact. Far more serious can be the potential loss of production, environmental damage, regulatory violation, or compromise to the safety of an operation. The latter may have ramifications beyond the targeted company; it may grievously damage the infrastructure of the host region or nation.

Worldwide, an increasing percentage of the population has become computer literate, and malicious hacking, in addition to being a nefarious hobby with high-profile news coverage, has become a means to profit financially. In fact, tools to automate malicious hacking are now publicly available on the Internet. Instances of computer virus attacks are increasing in frequency. External threats of terrorist, expert hackers and nation states are not the only concerns; knowledgeable insiders with malicious intent or even an innocent unintended act can pose a serious security risk to an industry or critical infrastructure. Combining all these factors, it is easy to see that the probability of someone gaining unauthorized or damaging access to a control system has increased.

While technology changes such as standardization, vertical connectivity, and remote access (both wire and wireless), as well as partner relationships may be good for the business, economics, efficiency and productivity ends of the critical infrastructure industries, they increase the potential risk for compromising the cyber security of IACSs. Likewise, as threats to industry increase, so does the need for cyber security.

The working group that authored this technical report determined that there were several categories of tools, countermeasures and technologies available for securing an IACS network. Major categories are covered in Clause 5 through Clause 10 of this technical report. The information in each clause provides an overview of each technology, tool and/or countermeasure category, a list of specific types of applications within that category and a discussion of how well that type of application fits the IACS environment and requirements.

IACS networks use many of the same computers and communication technologies as corporate IT/enterprise networks, because it is more economical to add to existing technologies than to start from scratch. However, unique technical and operating constraints shall be considered when applying security technologies. One of the major goals of this technical report is to highlight those areas that warrant special consideration of IACS factors.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

## 5 Authentication and authorization technologies

### 5.1 General

The concept of authorization has existed for as long as humans have had assets worth protecting. Authorization is the initial step in protecting an IACS system and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system. Once this information is determined, defence-in-depth access control measures can be implemented to verify that only authorized people and devices can actually access an IACS system. The first measure is usually authentication of the person or device that is attempting access to an IACS system.

Authorization can be as granular as determining access to specific files in an application or as encompassing as access to an entire enterprise or IACS network. Authorization is usually implemented indirectly via configuration tools provided by the vendors of operating systems,

applications and networks. Authorization mechanisms show up in virtually all systems and impose great architectural and administrative challenges at all levels of enterprise and IACS computing.

Authorization and authentication are fundamental to access control for an IACS. They are distinct concepts but are often confused because of the close relationship between the two. Proper authorization is, in fact, dependent upon authentication.

Authentication describes the process of positively identifying potential network users, hosts, applications, services and resources using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions. Based on the response received, the system may or may not allow the potential user access to its resources.

There are several possible factors for determining the authenticity of a person, device or system. For example, the test could be something known (e.g. PIN or password), something owned (e.g. key, dongle or smart card), something physical (e.g. biological characteristic such as a fingerprint or retinal signature), a location (e.g. global positioning system (GPS) location access), the time a request is made, or a combination of these attributes. In general, the more factors that are used in the authentication process, the more robust the cyber security process will be. When two or more factors are used, the process is known generically as multi-factor authentication.

There are two components to authentication:

- User authentication—traditional computer authentication such as “logging into a computer” or activating a human machine interface (HMI) to adjust a process.
- Network service authentication—the ability for networked devices to distinguish between authorized and unauthorized remote requests for IACS data or to perform actions on the IACS.

Computer systems in the IACS environment typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are often easy to guess or infrequently changed, and create additional security risk as a result. At the current time, protocols used in IACS environments generally have inadequate or no network service authentication.

NOTE Network service authentication should not be confused with “message authentication,” which is frequently used in security literature. Message authentication deals with protecting a message from modification during transmission and signing digital records for long-term electronic storage. This concept is included in Clause 7.

Listed below are several types of authentication and authorization technologies. Clause 9 on operating systems associated with IACS systems also includes a discussion of authorization issues.

### 5.2 Role-based authorization tools

#### 5.2.1 Overview

Role-based access control (RBAC) is a technology and tool that is attracting a great deal of attention because of its potential for reducing the complexity and cost of security administration in networks with large numbers of intelligent devices like some IACS systems. Under RBAC, security administration is simplified by using roles, hierarchies, and constraints to organize user access levels. RBAC reduces costs within an organization because it accepts that control operation employees change more frequently than the duties within positions.

#### 5.2.2 Security vulnerabilities addressed by this technology

RBAC systems are designed to minimize the potential for security violations by providing greater control over users’ access to information and resources of multiple devices in an IACS network. The level of control room operator access can take several forms, including viewing,

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

using, and altering specific IACS data or device functions. The promise of RBAC is a uniform means to manage access to plant floor devices while reducing the cost of maintaining individual device access levels and minimizing errors.

The traditional approach to controlling access to IACS information and network resources is to establish specific permissions for each user. Permissions are then configured into the security level mechanisms supported by the individual intelligent devices. An industrial control system may have thousands of devices, such as DCSs, HMIs, process historians, PLCs, motor control centres, smart sensors and application-specific data concentrators. While effective in a static environment, this approach is difficult to manage in dynamic environments where users enter and leave employment and contractors, original equipment manufacturers, system integrators, and vendors come and go. The constant stream of changes requires frequent updates to access permissions, a time-consuming and error-prone process. A common security lapse with this approach is that timely permission updates are not made, enabling unauthorized users (such as terminated employees) to access restricted functions. Quite often, plants either do not use or simply disable individual device security access levels for this reason.

RBAC addresses this problem by basing access on a user's role or job responsibilities rather than customizing access for each individual. For example, machine operators may be able to view certain files, but not alter them.

On the surface, basing access control on job descriptions may seem a bit restricting, but RBAC can grant multiple access permissions to groups and has the ability to grant elevated access privileges to certain individuals. Using the previous example, the machine operators could view files on a number of devices, but the machine vendor's support engineers could access additional functions only on their specific machine. Roles can also be set up based on location, projects, schedule, and management level.

Although employee and contractor turnover make it difficult to maintain individual permissions, it is not a problem for roles because they usually do not change as often. Being able to add or remove users from role groups in a centralized database minimizes the effort to keep access levels current and reduces the potential for error.

### 5.2.3 Typical deployment

Access to computer system objects in an IACS is based on a user's role in an organization. Users are associated with roles and roles are associated with permissions. Users have permission to access an object only if the user has an authorized role associated with that permission.

RBAC tools provide graphical user interfaces that simplify the process of establishing roles, groups and permissions. These tools are often Web-based and can be operated over an enterprise's corporate Intranet. Most RBAC tools centralize the repository of authorizations, while delegating the actual role assignment to the functional department manager. A plant might use RBAC to centralize access control to the intelligent devices of the control system, but assigning personnel to roles becomes the separate responsibilities of the instrumentation, maintenance, and operations support departments.

RBAC tools can set, modify, or remove authorizations in applications, but they do not replace the authorization mechanism; they do not check and authenticate users every time a user wants to access an application.

### 5.2.4 Known issues and weaknesses

In order to provide uniform authorization management, RBAC tools shall be able to work with the tokens, digital certificates, directories, or other authorization mechanisms of the intelligent devices they are protecting. RBAC tools offer interfaces to authorization mechanisms for most current platforms in the IT arena. However, legacy IACS systems or specialized IACS equipment require development of specialized interface software. Software development can pose an enormous task for many systems, and is the single largest reason that prevents many

IECNORM.COM : Click to view the full PDF of IEC TR 62443-3-1 ed 1.0:2009

companies from implementing single-sign-on capabilities to enterprise networks. This issue is a large problem for industrial control systems that use a number of proprietary operating systems or customized operating system implementations and interfaces.

Centralized RBAC strategies have the potential for making access to the control systems dependent upon the health and availability of the corporate wide area network and some central RBAC server. Thus, centralized RBAC introduces additional points of failure that can impact the availability of the industrial automation and control system. Another issue with RBAC is that it is a relatively new methodology whose benefits and applications are not yet well understood. Also, some IACS architectures do not presently support the methodology.

#### 5.2.5 Assessment of use in the industrial automation and control systems environment

At the time this technical report was released, the working group that authored it was not aware of any broad-based RBAC tools specifically developed for industrial control systems. In particular, tools that uniformly authorize control systems employing products from multiple vendors were not available. However, some equipment vendors did offer tools that centralize authorization of a portion of their products, such as access to the program development applications for controllers.

#### 5.2.6 Future directions

Protocols used in industrial environments will need to accommodate access control mechanisms consistent with RBAC. While difficult to achieve in many legacy protocols, this is occurring in some more modern protocols. One example of this is the OLE® for Process Control (OPC®) standard, which has developed security specifications for access control to OPC® servers.

Products that perform some measure of uniform authorization management for industrial control devices were introduced as early as 2005, but are not widely deployed. The functionality in these products may be incorporated into security gateways that combine a number of security functions.

#### 5.2.7 Recommendations and guidance

In the absence of uniform authorization tools, most designers of IACSs take precautions to minimize the amount of external traffic to and from the control system. While various architectural measures attempt to stop data flow into the control system from the enterprise systems, this cannot be achieved in total. While RBAC may increase the safety of spontaneous data requests to the control system, it is not a panacea for careless design of the data flows.

#### 5.2.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [NIST02]
- [FKC]
- [KG]
- [*b*hold]

### 5.3 Password authentication

#### 5.3.1 Overview

Password authentication technologies determine authenticity based on testing for something the device or the control operator that is requesting access to the IACS should know (i.e., a secret), such as a personal identification number (PIN) or password. Password authentication schemes are the simplest and most common.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1:2009

There are three general types of passwords:

- passcode or PIN—a short sequence of numbers used as the secret (e.g., the digits 1234);
- password—a short character string used as the secret (e.g., “hat34slow”);
- passphrase—a long string used to generate the secret (e.g., the phrase “downtown 23 boats hit cars and blew smoke into cabbage” might generate the secret radix-64 value X34B3-By88e-P345s-56df0).

Each password type follows the same concept, but provides different levels of complexity for the user and therefore the security for the system.

- A passcode is simple enough for even the smallest embedded device to manage. It often represents a number from 0 to 9999 and can be stored as a simple 16-bit integer. It is also the least secure method. The two most common examples are a PIN for an automatic teller machine card or the keypad on a door access device.
- A password is a longer secret, often in the 6 to 14 character range. It takes more memory and processing to manage, and therefore provides a little more security.
- A passphrase is a longer secret that could be used to create a numeric key for a cipher system. While it takes some effort to remember a phrase like “downtown 23 boats hit cars and blew smoke into cabbage,” it is much easier for most people to remember than the code “X34B3-By88e-P345s-56df0.” This method also provides more security because it is the hardest for a hacker to guess and is less probable for a password/code-breaking program to break.

### 5.3.2 Security vulnerabilities addressed by this technology

In the IACS environment, passwords can be used to limit requests for services and functions to authorized users.

### 5.3.3 Typical deployment

Passwords are commonly employed in one of two ways:

- The password is submitted with the request for authorization. Network service requests usually include the password with the request. A common example is a Simple Network Management Protocol (SNMP) request that includes a community name.
- After the request, the system requests the password to confirm authorization. User authentication generally requests the password after a user attempts access.

### 5.3.4 Known issues and weaknesses

The strength of a password is directly related to its length and entropy (randomness). The importance of length is fairly obvious. A two-digit passcode has only 100 possible values from 00 to 99, while an 8-character password has billions of possible values.

Entropy is a measure of the randomness in the password and is equally important. Passwords that use predicable sequences of digits (e.g., “1234”) or common English language words (e.g., “password” or “operator”) are far easier to predict than more random passwords. Unfortunately, the greatest weakness in the use of passwords is that control system users tend to pick passwords that are easy to remember and thereby have very low entropy and are easy to predict.

Most passcodes on a 12-key keypad end up as a simple physical pattern, like 1254 or 1478, while many computer passwords are birth-dates or a spouse or pet name. Cracking schemes use human preferences for pattern recognition and familiarization to allow attackers to guess the correct password in far fewer than the theoretical number of tries. Password vulnerability can be reduced if the vendor implements an active password checker that prohibit weak, recently used, or commonly used passwords.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

Another weakness is the ease of third party eavesdropping. Passwords typed at a keypad or keyboard are easily observed or recorded, especially in areas where attackers could plant tiny wireless cameras or hardware keystroke sniffers. Network service authentication often transmits passwords as plaintext (unencrypted), allowing any network capture tool to expose the actual password.

An improvement over plaintext passwords is hashed passwords. A one-way algorithm is used to cryptographically convert passwords into a hash code, which is extremely computationally expensive to decrypt back to the original password. However, not all hashed passwords are safe. It is possible to determine another password that hashes to the same value, but it is also computationally expensive to do so. More seriously, even if passwords are sent as cryptographic hashes, network capture tools often allow the message to be modified and "replayed," easily creating a new message complete with valid encrypted password without ever knowing the original password.

Password files shall be protected from read or copy access. One common method for password cracking is to copy the password file and run off-line programs against the file. These programs generate a large number of possible passwords and hashes, each with the same one-way algorithm, to build a password versus hash list. The program then compares the captured password files to the list until a match is found. This method of attack limits the exposure of the attacker and may result in a fully compromised system.

### 5.3.5 Assessment of use in the industrial automation and control systems environment

One problem with passwords unique to IACS environments is that a user's ability to recall and enter a password may be impacted by the stress of the moment. During a major crisis when human intervention is critically required, an operator may panic and have difficulty remembering the password and either be locked out completely or delayed in being able to respond to the event. If the password has been entered wrong and the system has a limit on allowed wrong password entries, the operator may be locked out permanently until an authorized employee can reset the account.

Special consideration shall be made when using IT policies based on login password authentication within the IACS environment. Without an exclusion list based on machine identification (ID), non-operator logon can result in policies being implemented such as auto-logoff timeout and administrator password replacement that can be detrimental to the operation of the system. Some controller operating systems make setting secure passwords difficult, as the password size is very small and the system usually allows only group passwords at each level of access, not individual passwords.

Some industrial (and Internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted systems.

### 5.3.6 Future directions

Industrial automation and control systems equipment should be sophisticated enough to allow high-level password security. IACS equipment needs to have protocols that allow passwords to be transmitted in secure ways (i.e., not plaintext). One method of password use for the future may well be a common method noted as RBA, or role-based authentication, where several operators have, in some cases, the same password and therefore are equally authorized since they all have the same authorities in relation to what they can or cannot do once they enter the control system through authorization. Such role-based methods associate the person with his or her job role as opposed to his or her individuality and are useful for administration in an environment where job roles change more frequently than in a common IT enterprise.

Future IACS password equipment and protocols shall be able to provide flexibility to an operator for various emergency situations. For instance, in an emergency situation, a panicked

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

operator may attempt to log in unsuccessfully several times. Not allowing the operator access to the system in an emergency situation could create severe problems with disastrous results. Therefore, there shall be provisions for the password algorithm to recognize the unsuccessful attempts of someone who has knowledge of the password through the use of the similarities of each of the unsuccessful attempts. The algorithm should then allow a simple emergency password to be used by the operator for logon purposes.

### 5.3.7 Recommendations and guidance

The following are general recommendations and considerations with regards to the use of passwords. Specific recommendations will be presented in IEC 62443-2-1[2].

- Passwords should have appropriate length and entropy characterization for the security required. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
- Initial passwords and passwords that have been reset should be securely transmitted to the intended receiver. User authentication not subject to social engineering methods shall be employed. These can include face-to-face ID authentication and voice-mail delivery.
- Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out during critical events.
- The keeper of master passwords should be a trusted employee, available during emergencies. Authority to change higher-level passwords should be limited to trusted employees. A password log, especially for master passwords, should be maintained separately from the control systems, possibly in a notebook locked in a vault or safe.
- In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), users should consider supplementing password authentication with other forms of authentication such as challenge/response or two-factor authentication using biometric or physical tokens.
- For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of strong encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner.
- For network service authentication purposes, passwords should be avoided if possible. There are more secure alternatives available, such as challenge/response or public-key authentication.

### 5.3.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [AGA-12]
- [NIST03], [NIST04], [NIST07], [NIST07A], [NIST07B], [NIST09], [NIST10]
- [IAONA]
- [Mix]
- [Zur]
- [Har1]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

[2] To be published.

### 5.4 Challenge/response authentication

#### 5.4.1 Overview

Challenge/response authentication requires that the service requester, the IACS operator, and service provider know a “secret” code in advance. When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider. If the response is as expected, it proves that the service requester has access to the “secret” without ever exposing the secret on the network.

#### 5.4.2 Security vulnerabilities addressed by this technology

Challenge/response authentication addresses the security vulnerabilities of traditional password authentication. When passwords (hashed or plain) are sent across a network, a portion of the actual “secret” itself is being sent. Giving the secret to the remote device performs authentication. Therefore, traditional password exchange always suffers the risk of discovery or replay. Because the secret is known in advance and never sent in challenge/response systems, the risk of discovery is eliminated. If the service provider can never send the same challenge twice, and the receiver can detect all duplications, the risks of network capture and replay attacks are eliminated.

#### 5.4.3 Typical deployment

Common challenge/response systems are:

- PPP-CHAP Internet Engineering Task Force (IETF)/RFC1994—PPP-CHAP allows a remote client to connect over a serial or dial-up link to a server. The client shall still know the password, but CHAP uses a challenge/response system to verify the password without sending it across the serial line where an attacker may see or replay it.
- Kerberos IETF/RFC1510—Kerberos is a centralized server system designed for small, single-authority networks. It allows servers to provide service to clients based on a simple, secure “ticket” concept. A theoretical example is an Object Linking and Embedding (OLE®) OPC® server that obtains a data read ticket from a central Kerberos server and submits it to a PLC before the PLC will answer data requests. Both Windows® and UNIX®/Linux® have options for Kerberos support.

#### 5.4.4 Known issues and weaknesses

- Challenge/response authentication cannot be used directly for user authentication because users are not willing to manually combine their passwords and a challenge to calculate a suitable response. Protocols like PPP-CHAP get around this problem by directly accepting the user’s password and managing the challenge/response authentication indirectly without direct user awareness. However, this hybrid approach still provides a way for determined attackers to observe keystrokes as the user enters them.
- A theoretical weakness in challenge/response authentication is that an attacker is provided with both the challenge and the response to examine off-line. If a known algorithm and key are used to create the response, an attacker can use this knowledge to calculate the “secret.” This vulnerability is easily avoided by using strong cryptographic algorithms that make reverse calculation difficult and time-consuming.
- The greatest weakness in challenge/response authentication for network service authentication lies in any system that allows a “roll-back attack” during some form of authentication negotiation. In a rollback attack, the attacker causes the service provider to agree to use a weaker legacy authentication method, such as plain text passwords or no authentication at all. This vulnerability can be avoided if the vendor provides methods to prevent rollback, such as a setting in the service device to restrict network service authentication to use only secure versions of the protocol, and the user enables those methods.
- Passwords, keys, or secrets used by challenge/response authentication shall be distributed somehow, either physically or by a network, which risks exposing them and compromising

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

the system. Distribution methods require special care in design and implementation to avoid becoming the weak link in the security system.

#### 5.4.5 Assessment of use in the industrial automation and control systems environment

For user authentication the direct use of challenge/response authentication is not feasible for control systems due to the possible latency that may be introduced in the necessary fast dynamics required for access to a control system or industrial network.

For network service authentication, the use of challenge/response authentication is preferable to more traditional password or source identity authentication schemes.

#### 5.4.6 Future directions

Industrial automation and control systems equipment and their protocols should be sophisticated enough to allow challenge/response authentication in order to provide for proper security in the future. When ordering these systems, one should look for a good and timely challenge/response authentication protocol such as the Challenge Handshake Authentication Protocol (CHAP), which authenticates using a challenge/response method. CHAP is used the same way as is Password Authentication Protocol, but CHAP provides a higher degree security. CHAP can be used by remote users, routers, and network access servers to provide authentication before providing connectivity.

#### 5.4.7 Recommendations and guidance

Challenge/response authentication provides more security than encrypted passwords for user authentication across a network.

Managing master encryption algorithms and master passwords becomes increasingly more complex as more parties are involved in the security processes, and is an important consideration in the robustness of the security scheme.

#### 5.4.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Sim]
- [ZC]

### 5.5 Physical/token authentication

#### 5.5.1 Overview

Physical or token authentication is similar to “password authentication,” except that these technologies determine authenticity by testing for a device or token the person requesting access should have in his or her possession, such as security tokens or smart cards. Increasingly, PKI keys are being embedded in physical devices such as the universal serial bus (USB).

Some tokens support single-factor authentication only, so that simply having possession of the token is sufficient to be authenticated. Others support dual-factor authentication that require knowledge of a PIN or password in addition to possessing the token in order to be authenticated.

#### 5.5.2 Security vulnerabilities addressed by this technology

The primary vulnerability that token authentication addresses is the ability to prevent the secret from being easily duplicated or shared with others. It eliminates the all-too-common scenario of a password to a “secure” system being left on the wall next to the personal computer (PC) or

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

operator station. The security token cannot be duplicated without special access to equipment and supplies.

A second benefit is that the secret within a physical token can be very large, physically secure, and randomly generated. Because it is embedded in metal or silicon, it doesn't have the same risks as manually entered passwords.

If a security token is lost or stolen, the authorized user loses access, unlike traditional passwords that can be lost or stolen without notice.

### 5.5.3 Typical deployment

Common forms of physical/token authentications include:

- traditional physical lock and keys;
- security cards (magnetic, smart-chip, optical coding);
- radio-frequency devices in the form of cards, key-fobs, mounted tags;
- dongles with secure encryption keys that attach to the USB, serial, or parallel ports of computers;
- one-time-authentication code generators.

### 5.5.4 Known issues and weaknesses

For single-factor authentication, the largest weakness is that physically holding the token means access is granted (e.g., anyone finding a set of lost keys now has access to whatever they open). Physical/token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used along with the token.

Dual-factor authentication is an accepted good practice for high-security applications.

Tokens require logistical and financial support to issue, distribute, and administer. They typically also require additional servers to support authentication.

### 5.5.5 Assessment of use in the industrial automation and control systems environment

Physical/token authentication is an effective security technique and should have a strong role in IACS environments.

### 5.5.6 Future directions

Reliable and highly secure token solutions are available today. Tokens are becoming available in forms that are convenient to use, such as key-ring fobs and embedded functionality in photo ID cards.

### 5.5.7 Recommendations and guidance

Physical/token authentication has the potential for a strong role in IACS environments. An access card or other token can be an effective form of authentication for computer access, as long as the computer is in a secure area (e.g., once the operator has gained access to the room with appropriate secondary authentication, the card alone can be used to enable control actions). Where additional security is warranted, single-factor methods such as passwords can be combined with physical/token authentication to create a significantly more secure two-factor authentication system.

Where possible, ensure that the hardware implementation of the physical token is tamper-proof, such that any attempt to x-ray, reverse engineer, or tamper with the registers on the

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

physical token where the key and associated algorithms reside, renders the device useless by zeroing out all registers.

If physical/token authentication is deployed, it is important to include sufficient resources to manage issues regarding tokens, including token distribution, replacement and returns.

#### 5.5.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Har2]
- [Zur]

### 5.6 Smart card authentication

#### 5.6.1 Overview

Smart cards are similar to token authentication, but can provide additional functionality. Smart cards can be configured to run multiple on-board applications to support building access, computer dual-factor or triple-factor authentication, and cashless vending on a single card, while also acting as the company photo ID for the individual.

Typically, smart cards come in a credit card size form-factor that can be printed, embossed, and individually personalized. Smart cards can be customized, individualized, and issued in-house or outsourced to service providers who typically issue hundreds of thousands of cards per day.

#### 5.6.2 Security vulnerabilities addressed by this technology

Smart cards enhance software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets. They also:

- Isolate security-critical computations involving authentication, digital signatures, and key exchange from other parts of the system that do not have a need to know.
- Enable portability of credentials and other private information between multiple computer systems.
- Provide tamper-resistant storage for protecting private keys and other forms of personal information.

#### 5.6.3 Typical deployment

Smart cards can vary from simple memory cards to cards with complex on-board processing capabilities. Cards such as the Java® card even allow dynamic uploading of new applications, similar to the way that a web browser can run downloaded Java® code.

Card readers are available as USB, PC-card and RS232 devices, and are increasingly available built into devices such as keyboards and keypads. For the latter devices, some ensure that the PIN is never processed by the workstation but entered directly into the smart card. These “secure PIN entry devices” can prevent workstation-based key logger attacks on the PIN.

Smart cards can have metallic contacts, similar to those commonly found on today’s credit cards, or can have proximity radio capabilities that work up to a range of 1 m to 2 m.

Smart cards also provide the ability to combine several uses into a single card. For example, building access control, computer authentication, application authentication, and cashless vending can be integrated on a single card. When a user leaves a work area for lunch, he would have to take his card with him to purchase lunch (by cashless vending) or to return into

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

the secure area, ensuring that he removed his smart card from his computer, which would automatically lock it.

Smart card applications for computer authentication typically hold the user's credentials securely on the card. The user shall input a PIN to unlock the card and allow the credentials to be accessed. It is normal for applications to use a challenge-response mechanism between the computer and the card to allow the credentials to be retained only within the card and never transferred to the computer where they could be potentially compromised.

### 5.6.4 Known issues and weaknesses

Many smart cards offer high quality dual-factor authentication solutions that are robust enough for financial sector applications. The majority of issues are logistical around issuing the cards, particularly to replace lost or stolen cards. These include:

- A lost or stolen card may provide some level of access by the finder.
- Smart cards without the matching hardware and access control system are no better than non-smart cards.
- Lost or damaged smart cards can create a temporary block for access to the industrial automation and control system necessary for safety or general operations if backup cards have not been issued.
- If the smart card PIN is entered using the workstation, it can be vulnerable to attack if the workstation is compromised. Secure PIN entry devices that do not allow workstation access to the PIN can be used to mitigate this vulnerability.
- Using smart cards for multiple applications outside of the control system, such as cashless vending, creates potential for code access vulnerability.

There is also some concern that smart card security may be compromised using differential power analysis (DPA) techniques. DPA is performed by monitoring the electrical activity of a device, then using advanced statistical methods to determine secret information (such as secret keys and user PINs) in the device.

### 5.6.5 Assessment of use in the industrial automation and control systems environment

Although smart cards are relatively inexpensive and offer useful functionality in an industrial control system context, their implementation shall be done within the overall security context of the plant. The necessary identification of individuals, issuance of cards, revocation should compromise be suspected, and assignment of authorizations to authenticated identities, represent a significant initial and on-going challenge. In some cases, corporate IT or other resources may be available to assist in the deployment of smart card and public key based infrastructures.

### 5.6.6 Future directions

Smart cards are increasing in memory and processor capacity and flexibility. The cost of smart cards and smart card readers is likely to be reduced as financial services organizations adopt smart card technology for credit card use (as is beginning to happen in the United Kingdom). Integrating smart cards into standard IT product offerings is likely to follow, as credit card payment by smart card becomes the norm. Another possible future direction is integration into Web browsers to allow secure on-line retail transactions.

### 5.6.7 Recommendations and guidance

Smart cards should be examined for potential use in controlling access to IACS environments, both from a physical perspective and for access to computer systems.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

If smart cards are implemented in an industrial control setting, provisions for management of lost or damaged cards should be considered, as well as the costs to incorporate a respective access control system and provide a management process for card distribution and retrieval.

#### 5.6.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [anon39]
- [Jun]
- [Zur]

### 5.7 Biometric authentication

#### 5.7.1 Overview

Biometric authentication technologies determine authenticity by determining presumably unique biological characteristics of the human requesting access. Usable biometric features include finger minutiae, facial geometry, retinal and iris signatures, voice patterns, typing patterns, and hand geometry.

#### 5.7.2 Security vulnerabilities addressed by this technology

Like physical token and smart cards, biometric authentication enhances software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets. In addition, since biometric characteristics are supposedly unique to a given individual, biometric authentication addresses the issues of lost or stolen physical token and smart cards.

#### 5.7.3 Typical deployment

Common forms of biometric authentication include:

- fingerprint scanners;
- hand geometry scanners;
- eye (iris or retina) scanners;
- face recognition;
- voice recognition.

#### 5.7.4 Known issues and weaknesses

Noted issues with biometric authentication include:

- All biometric devices suffer from the need to detect a real object from a fake (e.g., how to distinguish a real human finger from a silicon-rubber cast of one or a real human voice from a recorded one).
- All biometric devices are subject to type-I and type-II errors (the probability of rejecting a valid biometric image, and the probability of accepting an invalid biometric image, respectively). In all cases, the user should attempt to implement biometric authentication devices that have the lowest crossover between these two probabilities, also known as the crossover error rate.
- Some biometric devices are environmentally sensitive. As a result, temperature, humidity, and other environmental factors can affect these devices.
- Biometric scanners are reported to “drift” over time and may need occasional retraining. Human biometric traits may also shift over time, necessitating periodic scanner retraining.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- Device training may require face-to-face technical support and verification, unlike a password that can be given over a phone or an access card that can be handed out by a receptionist.
- Temporary inability of the sensing device to acknowledge a legitimate user can prevent needed access to the control system.
- Some biometric authentication devices are more “socially acceptable” than others. For example, retinal scans are very low on the scale of acceptability, while iris scanners and thumbprint scanners are high on the scale of acceptability. Users of biometric authentication devices will need to take social acceptability for their target group into consideration when selecting among various biometric authentication technologies.

#### 5.7.5 Assessment of use in the industrial automation and control systems environment

Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token key or badge-operated employee time clocks increases the security level.

#### 5.7.6 Future directions

Biometrics is becoming more reliable and increasingly integrated into common IT components, such as keyboards. This trend is already progressing into hand-held items such as personal data assistants (PDAs) and mobile telephones.

Biometrics also combines well with smart card technology, which can hold biometric data about the user. When combined with a PIN, this provides three-factor authentication: something the presenter has, knows, and is.

#### 5.7.7 Recommendations and guidance

Biometrics can provide a valuable authentication mechanism, but needs to be carefully assessed for industrial applications because physical and environmental issues within the final installation environment may need to be restructured for reliable authorized authentication. The exact physical and environmental properties of an installation would have to be coordinated with a system vendor or manufacturer.

#### 5.7.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Har2], pp. 32-34
- [Teu], p. 106

### 5.8 Location-based authentication

#### 5.8.1 Overview

Location-based authentication technologies determine authenticity based on the physical location in space of the device or human requesting access. For example, these systems may involve using GPS technologies to ensure that the requestor is where he or she claims to be or is within an area known to be physically secure. Authentication may be done directly, so that physical access to a device implies authority, or indirectly, so that an ID or address representing the location is used to imply authority.

A small percentage of network service authentications currently performed in IACS environments are location based, where some form of identity directly (or indirectly) linked to the location is used to authenticate the user. A simple example is a control device that only accepts commands if the source address (such as an IP) of the command matches a preconfigured address assigned to the main control room.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 Ed 1.0:2009

System security fundamentally depends on the ability to authenticate users and control access to resources. Geodetic location, as calculated from a location signature, adds a fourth and new dimension to user authentication and access control. It can be used to determine whether a person is attempting to log in from an approved location, - e.g., a user's office building or home. If a user is mobile, then the set of authorized locations could be a broad geographic region (e.g., city, state, country). In that case, the login location serves to identify the place of login as well as to authenticate it. If unauthorized activity is detected, it will facilitate finding the individual responsible for that activity.

### 5.8.2 Security vulnerabilities addressed by this technology

User authentication mechanisms are based on information the user knows (e.g., password or PIN), possession of a device (e.g., access token or crypto-card), or information derived from a personal characteristic (biometrics). None of these methods is foolproof. Passwords and PINs are often vulnerable to guessing, interception, or brute force search. Devices can be stolen. Cryptographic systems and one-time password schemes can fail even when the algorithms are strong. Typically, their security reduces to that of PINs or passwords, which are used to control access to keys stored in files or activation of hardware tokens. Biometrics can be vulnerable to interception and replay. Another way to supplement the authentication and further reduce the vulnerabilities of passwords and pins of an IACS user, especially from a remote location, is to deploy location-based authentication.

### 5.8.3 Typical deployment

Using location-based authentication, the physical location of a particular user or network node at any instant is uniquely characterized by a location signature. This signature is created by a Location Signature Sensor (LSS) from the microwave signals transmitted by the twenty-four hour satellite constellation of the GPS. The technique is used by an independent device to determine the geodetic location (latitude, longitude, and height in a precisely defined geocentric coordinate reference system) of the LSS to an accuracy of a few meters or better. The signature and its derived location are virtually impossible to forge. An entity in cyberspace will be unable to pretend to be anywhere other than where its LSS is actually situated. When attempting to gain access to a host server, the remote client is challenged to supply its current location signature. The host, which is also equipped with an LSS, processes the client signature and its own simultaneously acquired satellite signals to verify the client's location to within an acceptable threshold (a few meters to centimeters, if required). For two-way authentication, the reverse process would be performed. Re-authorization can be performed every few seconds or longer.

### 5.8.4 Known issues and weaknesses

The use of location signatures has the potential of being used to track the physical locations of individuals who are using a mobile device. This technology also requires a hardware device at both the host and the client end, which adds costs.

### 5.8.5 Assessment of use in the industrial automation and control systems environment

This technology could be of great benefit in authenticating users, especially in enhancing wireless security within a plant site or a remote location. With very tight determination of location, it would be easily possible to limit access to users within a fairly tight geographical area and refuse connection or disconnect users outside of this area. With mobile users it would be easily possible to create access roles based on physical location changes. Different roles/capabilities could be allowed depending on the physical location of the user. Engineers on laptops who can make changes while working within the plant site could be restricted to a view-only access when off the plant site. This technology has much potential for enhancing the security of a control system.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

### 5.8.6 Future directions

Cost reduction and more vendors for this solution are required to increase the attractiveness of this technology. Technology also needs to be imbedded in mobile devices.

### 5.8.7 Recommendations and guidance

Web searches did not reveal resources for this solution.

### 5.8.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [DM]
- [anon04]

## 5.9 Password distribution and management technologies

### 5.9.1 Overview

User identification coupled with a reusable password, which is updated and changed in a policy-driven consistent manner, is the most common form of system identification and authorization mechanisms for control system operators and users. A password is a protected sequence of characters used to authenticate an individual. Authentication factors are based on what a user knows (e.g., a password), has (e.g., a smart card), or is (e.g., a biometric). A password is something the user knows.

Passwords are one of the most used authentication mechanisms employed today for control system access and, therefore, need to be highly protected. It is important that passwords are strong and properly managed and therefore distributed in a manner that is secure but also guarantees updates and changes to negate wrong disclosure, via carelessness from long-term consistent use.

### 5.9.2 Security vulnerabilities addressed by this technology

If passwords are properly generated, updated, and kept secret, they can provide effective security. Passwords are authentication based on what a user knows as opposed to something the control system user has or is.

### 5.9.3 Typical deployment

Passwords are used during the logon process from either a central control room, a remote location within the industrial organization or outside the industrial organization, and can be transferred via wireless or wire modes or a combination thereof.

### 5.9.4 Known issues and weaknesses

Although passwords are the most commonly used authentication mechanisms, they are also considered one of the weakest security mechanisms available. Their weakness stems from the facts that users usually choose passwords that are easily guessed, tell others their passwords, and many times write a password on a sticky note and may or may not hide it somewhere near the computer or HMI in the control room. To most control system users, security is usually not the most important or interesting part of using their computers and HMIs— until someone hacks into their computers and steals information or much worse, disrupts automated operation of a key control system asset.

In order to keep a system secure, passwords need to be kept confidential and routinely changed, altered, and even updated since attackers (insiders included) can try the following techniques to obtain a password and ultimately compromise security.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- Electronic monitoring: An attacker can listen to network traffic to capture information especially when a user is sending a password to an authentication server. The password can be copied and reused by the attacker at another time. Reusing the password is called a “replay attack.”
- Access the password file: Password files are usually located on the authentication server. The password file contains many users’ passwords and, if compromised, can be a source of a lot of damage. The password file should be protected with access control mechanisms and encryption.
- Brute force attacks: An attacker can use a tool that cycles through many possible character, number, and symbol combinations to uncover a password.
- Dictionary attacks: An attacker will use files of thousands of words to compare to the user's password until a match is found.
- Social engineering: An attacker falsely convinces an individual that the attacker has the necessary authorization to access specific resources.

#### 5.9.5 Assessment of use in the industrial automation and control systems environment

Passwords can be the strongest or weakest link in any access to industrial automation processes or control systems. Static passwords (passwords that stay the same for a period of time) are used in many situations where dynamic passwords are impractical. It is a wise idea to change static passwords periodically such as every week. Dynamic passwords (new password for each logon) offer better security and should be used when practical. For more information on dynamic passwords, see the next subclause.

#### 5.9.6 Future directions

Security will become more important in the future because of increased awareness of vulnerabilities and increased abilities of hackers. For instance, a hacker can increase his ability dramatically through new and more sophisticated tools being developed, such as key stroke logging programs embedded through a virus in the enterprise network and then in to the control LAN.

One strategy to increase security is to use one-time passwords. A one-time password is also called a dynamic password. A dynamic password is used for authentication purposes and is only good once. After the password is used, it is no longer valid; thus, if a hacker obtained this password, it could not be reused. This type of authentication mechanism is used in environments that require a higher level of security than static passwords provide.

There are two general types of one-time password generating tokens: synchronous and asynchronous. Each is described below. The token device generates the one-time password for the user to submit to an authentication server.

The token device, or password generator, is usually a handheld device that has a liquid crystal display and possibly a keypad. This hardware is separate from the computer the user is attempting to access. The token device and authentication service need to be synchronized in some manner to be able to authenticate a user. The token device presents the user with a list of characters to be entered as a password when logging on to a computer. Only the token device and authentication service know the meaning of these characters. Because the two are synchronized, the token device will present the exact password the authentication service is expecting. This is a one-time password, also called the token, and is no longer valid after initial use.

A synchronous token device synchronizes with the authentication service by using time or a counter as the core piece of the authentication process. If the synchronization is time-based, the token device and the authentication service shall hold the same time within their internal clocks. The time value in the token device and a secret key are used to create the one-time password, which is displayed to the user. The user enters this value and a user ID into the computer, which then passes them to the server running the authentication service. The

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

authentication service decrypts this value and compares it to the value that it expected. If the two match, the user is authenticated and allowed to use the computer and resources.

If the token device and authentication service use counter-synchronization, the user will need to initiate the logon sequence on the computer and push a button on the token device. This causes the token device in the authentication service to advance to the next authentication value. This value and a base secret are hashed and displayed to the user. The user enters this resulting value along with a user ID to be authenticated.

In either time-based or counter-based synchronization, the token device and authentication service shall share the same secret base key used for encryption and decryption.

A token device that is using an asynchronous token-generating method uses a challenge-and-response scheme to authenticate the user. In this situation, the authentication server sends the user a challenge, which is a random value also called a nonce. The user enters this random value into the token device, which encrypts it and returns a value that the user uses as a one-time password. The user sends this value, along with a user name, to the authentication server. If the authentication server can encrypt the value, and it is the same challenge that was sent earlier, the user is authenticated.

Both synchronous and asynchronous token systems can fall prey to masquerading if a user shares his identification information and the token device is shared or stolen. The token device can also have battery failure or other malfunctions that would stand in the way of a successful authentication. However, a system using a token device is not vulnerable to electronic eavesdropping, sniffing, or password guessing.

### 5.9.7 Recommendations and guidance

The degree of security needs to be consistent with the value of the information and the process, and especially for control systems, with the critical industrial assets and equipment that it protects. Small, stand-alone control systems that do not contain valuable information or that are connected to insignificant benign assets, do not control valuable processes, and are not connected to the Internet can be protected with simple passwords. On the other hand, systems that are interconnected, contain valuable information, control a valuable process, or control valuable and dangerous processes and equipment, need to have more sophisticated password security. In this case, cognitive passwords and one-time passwords are appropriate and, over the long term, cost-effective. In a compensated process, one hacker intrusion could result in millions of dollars in lost revenue, severe damage to systems and products, loss of confidential information, and harm to personnel and the environment.

### 5.9.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Har1]
- [anon29]

## 5.10 Device-to-device authentication

### 5.10.1 Overview

Device-to-device authentication ensures that malicious changes to data traveling between two devices can be recognized. Authentic data are those that have been verified as authentic by the originating device, and have been validated as authentic by the receiving device. Device-to-device authentication does not prevent malicious tampering of data, but it will denote when data have been modified. Authentication can apply to the data traveling between devices, to the identity of users sending and receiving data, to the type of application sending data, to sessions between devices, and any combinations of these.

IECNORM.COM : Click to view the full PDF of IEC TR 62443-3-1 ed1.0:2009

Strong authentication is typically defined by combining two of the following methods from "something you have," "something you know," and "something you are." These are considered to be the most secure form of authentication.

The communication layers can include a variety of styles of physical layer and protocols including wired and wireless, serial based and IP based.

NIST[3] defines four levels of authentication using tokens, ranging from data authentication only, to data and identity authentication, to data and identity authentication with soft encrypted or revolving tokens, to data and identity authentication with hard encrypted tokens. Note that none of these types of authentication requires the data being sent to be encrypted. Only the last two types require the token to be encrypted along with the unencrypted data.

### 5.10.2 Security vulnerabilities addressed by this technology

Device-to-device authentication mitigates vulnerabilities associated with data integrity. Confidentiality of data is not addressed by this technology. In most cases, the availability of data will be higher if only authentication and integrity protection is applied since this technology does not rely on the encryption of the data. Overheads related to authentication and integrity protection are typically lower than those needed for confidentiality protection.

Authentication technology will prevent any entity without the proper token from sending authentic data, regardless of the data content (e.g., data could be telemetry, firmware, files, SCADA commands, or other). Thus, man-in-the-middle attacks are mitigated by this technology.

If the authentication of data occurs at a device's application layer, then authentication technology will prevent some forms of attacks focused at corrupting the data before it is sent. If the authentication validates the user's identification (such as biometric devices), then this technology is further beneficial.

### 5.10.3 Typical deployment

Device-to-device authentication is often deployed in conjunction with encryption. However, many control system users, such as those in the electric power industry, do not need the confidentiality that is gained with encryption, but rather need only data integrity and the ability to troubleshoot with clear text. For these types of users, authentication of data (and possibly the user) provides a very good solution. For devices that do not have users, authentication of the application can be performed in lieu of the user.

### 5.10.4 Known issues and weaknesses

Device-to-device authentication will not mitigate denial of service attacks.

Advanced man-in-the middle attacks, where clandestine hackers passively sniff network traffic, gain access codes and addresses, then inject a malicious attack, are only hindered by authentication technologies.

Authentication should not be confused with authorization (access privileges granted by an entity), nor does it include role-based access control (e.g., group memberships).

### 5.10.5 Assessment of use in the industrial automation and control systems environment

Authentication technologies have been widely used within Transmission Control Protocol/Internet Protocol (TCP/IP) based networks. However, many protocols in the IACS

---

3 *Glossary of computer security terminology*, U.S. National Institute of Standards and Technology, 1991.

IECNORM.COM : Click to view the full PDF of IEC TR 62443-3-1 ed 1.0:2009

environment are not IP based and require specific implementations of authentication. Utility industries such as natural gas and electric power are currently pursuing security solutions to their communications, which include authentication.

#### 5.10.6 Future directions

Several groups are currently working on solutions to control system security. IEC TC57 has been tasked with securing IEC 60870-5 protocol and DNP3 protocols, which are prolific within the electric power utility industry. The American Gas Association is finalizing its specification, AGA-12, requiring both cryptographic and authentication technologies.

It is apparent that manufacturing and utility communications are requiring integrated security. For many controls applications, confidentiality is not required, and therefore authentication is a good security solution. Issues surrounding key (or token) management technologies will become prevalent as authentication solutions are integrated.

#### 5.10.7 Recommendations and guidance

Users should adhere to vendor best practices to ensure proper device-to-device authentication deployment.

#### 5.10.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [AGA]
- [TC57]
- [DNP]
- [NIST12]

## 6 Filtering/blocking/access control technologies

### 6.1 General

Access control technologies are filter and blocking technologies designed to direct and regulate the flow of information between devices or systems once authorization has been determined.

Firewalls are the most commonly used form of this technology.

### 6.2 Network firewalls

#### 6.2.1 Overview

A firewall is a mechanism used to control access to and from a network and protect attached computers from unauthorized uses. Firewalls enforce access control policies using mechanisms that either block or permit certain types of traffic, thus regulating the flow of information.

Firewalls typically block traffic from the outside of a protected area to the inside of a protected area, while permitting users on the inside to communicate with outside services. There are also other, more restrictive configurations that restrict external access from within a protected network. More restrictive policies are also possible and likely to be appropriate in an IACS context. While it is important to have a firewall separating a company's enterprise network from the Internet, it is even more important to have firewalls between the enterprise network and industrial automation and control systems LANs. Additionally, the best cyber security practice is to have the servers that the control system LAN needs to access on the enterprise network be placed between firewalls in a demilitarized zone (DMZ) arrangement.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

There are three general classes of firewalls:

- Packet filtering: This type of firewall checks the address information in each packet of data to a set of criteria before forwarding the packet. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. The advantages of packet filtering firewalls include low cost and low impact on network performance, usually because only the source address in the packet is examined. For example, the IP source address of each packet is identified, then an established rule determines if the packet should be discarded or forwarded. This method is also sometimes called s*tatic filtering*.
- Stateful inspection: Stateful inspection firewalls filter packets at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the application layer. Stateful inspection keeps track of active sessions and uses that information to determine if packets should be forwarded or blocked. It offers a high level of security, good performance, and transparency to end users, but is expensive. Due to its complex nature, it can be less secure than simpler types of firewalls if not administered by highly competent personnel. This method is also sometimes called d*ynamic packet filtering*.
- Application proxy: This type of firewall examines packets at the application layer and filters traffic based on specific application rules, such as specified applications (e.g., browsers) or protocols (e.g., file transfer protocol (FTP). It offers a high level of security, but has a significant impact on network performance. It is not transparent to end-users and requires manual configuration of each client computer.

### 6.2.2 Security vulnerabilities addressed by this technology

A growing need exists for communication between process control networks and the outside. Typically, the communication is one-way, thus transferring process data out. A firewall is an efficient and well-known device to be used to enforce security in the data communication process. As Figure 1 indicates, a firewall provides security protection for the IACS environment by executing the following actions:

- limiting data from/to the process control network;
- logging successful and unsuccessful transactions through the firewall;
- enabling networks to interact that are not designed to do so (routing/NAT).

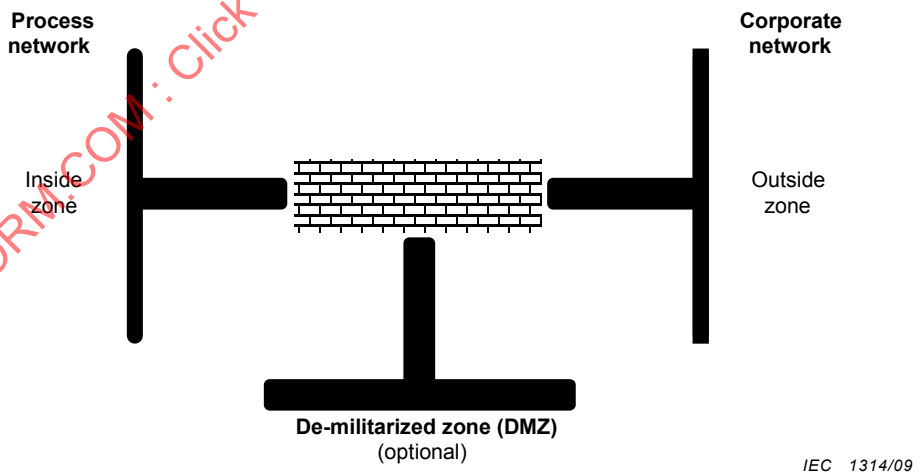


**Figure 1 – Firewall zone separation**

Limiting data from/to the process control network can be configured in several ways. The more sophisticated firewalls have the ability to filter by a combination of:

- IP-addresses (or IP-segments) on the outside allowed on the inside and vice versa;

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

- ports allowed for communication;
- applications allowed for communication.

Although not typical in control systems, intrusion detection systems (IDS) may be installed and firewalls connected enabling an IDS-system to respond to a security threat, for instance, by blocking firewalls, resetting sessions or dropping traffic that matches an attack signature. An intrusion detection system monitors either traffic patterns on the network or files in host computers, looking for signatures that indicate an intruder has or is attempting to break into a system.

### 6.2.3 Typical deployment

Firewalls can be implemented at several levels of the total network in a company. Firewalls are an integrated part of the company's IT security strategy; thus, brand and models are depicted from a central organization.

Firewalls used in IACS environments often protect a physical area (i.e., factory or building), but should be used taking into account the infrastructure and data communication. If set up improperly (i.e., in the wrong position in the network), firewalls are worthless because the firewall has to be configured with an insecure filter in order for a business to operate.

### 6.2.4 Known issues and weaknesses

Firewalls are not a solution to all intrusion problems in an IACS. Some of the known weaknesses in relying only on firewalls include:

Firewalls are not designed for process industry applications (DCS, SCADA), making it difficult to tailor the filtering for optimal security. In IACSs, firewalls should not be used as a single means of protection. Software and hardware firewalls should be used in connection with other security measures such as IDS-systems, monitoring systems such as netIQ/MOM, and computer software such as Active Directory and VPN (Virtual Private Network).

Firewalls have evolved and become increasingly complex, sometimes requiring specialized expertise for each different brand or model.

Reviewing logs (maintenance) is a tedious and time-consuming task. Central monitoring systems have eased that work.

Patching firewalls (maintenance) is as important as patching servers and clients on a network.

### 6.2.5 Assessment of use in the industrial automation and control systems environment

Firewalls should be used as an important tool to ensure security. The application and configuration of firewalls should be balanced against the perceived security threat and the likely impact in case a security exploit is used. As is the case with other complex technologies, it is important to start simply and logically with the greater perspective in mind. Specifically, configuration of firewalls should start with setting up the firewall configuration to deny all traffic, and then looking at the traffic required and only allowing it explicitly.

The effort required for operation of firewalls should also be considered. Level of expertise, complexity and stability of traffic through a firewall, and past experience are important factors to keep in mind when determining the appropriate level of security.

The DMZ can be an efficient place to put servers that communicate with the outside.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0 2009

### 6.2.6 Future directions

Firewalls are a necessary tool to ensure security when there is a need for direct data communication between networks. Hardware firewalls are preferred as the primary security component, since they are more secure than software firewalls.

In newer Windows® operating systems such as “Vista”, software firewalls are built in to the operating system, which make security configuration on clients and servers easier and more efficient.

### 6.2.7 Recommendations and guidance

Recommendations are to use hardware firewalls from recognized vendors (i.e., use a limited number of models), as well as knowledgeable, dedicated personnel to set up and operate firewalls.

Configuration of a firewall should be in compliance with the following guidelines:

- Traffic between the zones or networks connected to the firewall is generally closed (stateful event).
- The firewall should only be open for traffic from the process control network to the administrative network, or the DMZ. No traffic should be allowed directly from the administrative network into the process network.
- There is only open traffic from the DMZ to the administrative network and selected servers on the process control network.
- There is only open traffic from the administrative network in the building (IP-segment) to the DMZ and selected servers on the process network.
- Never allow traffic to and from the whole process control network, but only from the administrative network; and only allow traffic from the needed servers.
- Never allow traffic from the process control network to the Internet.
- Network components on the process control network can be managed centrally.
- Secure the management interface with appropriate authentication measures.
- Remove default passwords.

Operation of a firewall should be done according to written instructions and should include:

- review of logs;
- review of the firewall configuration setting frequently for adequacy;
- patching of firewall operating system (OS).

### 6.2.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [IATF]
- [CR]
- [Cor]
- [Far]
- [NISCC]
- [IAONA]
- [NIST03], [NIST10]
- [Mix]
- [DNvHC]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- [anon06]
- [Pol]
- [GGM]
- [Wool], pp. 459-468
- [SP]
- [GJ]
- [LB], pp. 363-371
- [XL], pp. 3296-3300
- [anon01]
- [CG], pp. 328
- [Har02], pp. 48-55, 58-63, 83, 89, 91
- [Teu], p. 73.
- [Zur], 6.3, 27.3.

## 6.3 Host-based firewalls

### 6.3.1 Overview

Host-based firewalls are software solutions deployed on a workstation or controller to control traffic that enters or leaves that specific device. This type of firewall enforces a local access control policy by either blocking or permitting certain types of traffic at the network interface card or IP stack level before presenting the packet to other applications running on the host.

### 6.3.2 Security vulnerabilities addressed by this technology

A host-based firewall on a computer system serves the same purpose as a lock on a filing cabinet. It protects a specific computer from unauthorized communication from applications or users on other systems. It can also be used as a low-cost protection mechanism for computers connected directly to the Internet, such as VPN-capable laptops and PDAs, but is more commonly used for home or small business environments.

Some vendors offer host-based firewalls that act as host intrusion detection systems. These offerings include simplified clients that serve as personal firewalls on the personal computer with advanced options available for the server.

Tasks performed by host-based firewalls include:

- blocking inbound packets from being processed by applications on the device;
- controlling outgoing traffic from the host;
- recording information useful for traffic monitoring and intrusion detection.

### 6.3.3 Typical deployment

Host-based firewalls are installed on each machine to create a protected collection of computers with each machine having its own access rules. This protection method is typically intended as a last line of defence, protecting the workstation when all other defences have failed to block an unwanted packet.

Host-based firewalls have similar capabilities to network firewalls, including stateful packet inspection. They serve a complementary function to network firewalls on individual workstations, and protect application-level software from many DoS attacks by filtering out bad packets at the network interface card or TCP/IP stack level.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

### 6.3.4 Known issues and weaknesses

Host-based firewalls do not protect workstations against most data-driven attacks (i.e., viruses), some denial-of-service attacks, social engineering attacks, and malicious insiders. Similar to network firewalls, host-based firewalls cannot protect against tunnelling over allowed application protocols by infected or poorly written applications.

Firewalls tend to be viewed as a panacea, potentially providing a false sense of security when they should be looked at as one part of a larger network security approach. Firewall deployment does not remove the need to implement software controls on internal networks or proper host security on servers.

Firewalls will not help if an organization does not understand the kind of access it wants to allow or deny. Developing effective access control rules is a complex process that typically requires an IT professional specifically trained on network security issues.

### 6.3.5 Assessment of use in the industrial automation and control systems environment

In an IACS environment, host-based firewalls are still relatively rare, particularly on critical control devices or workstations. Most controller-based operating systems will not permit deployment of this type of software and some HMI vendors may prohibit using this type of software on their workstations to guarantee proper operation or to retain the warranty.

NOTE The host firewall compatibility issue is the result of many DCS vendors testing and validating their systems with a controlled set of applications on the HMI. A vendor may void its DCS warranty if a user adds software to the system because of the potential interference with critical systems. Improper software installation could also negate supplier liabilities.

Issues faced in deploying host-based firewalls in IACS environments include:

- The lack of firewall products available for non-IP based protocols such as Foundation Fieldbus®, Profibus®, or any serial-based network;
- The lack of host-based (software) firewall products available for typical controller-based operating systems found on PLCs, RTUs and DCSs;
- Some Windows® or UNIX® control system software packages may be incompatible with host-based (software) firewall products;
- The possible addition of latency to control system communications;
- The lack of experience in the design of filter rule sets suitable for industrial applications;
- Significant overhead is required to manage host-based firewalls in widely dispersed systems typical of SCADA environments.

This technology requires improved central administration and management of widely dispersed host-based firewalls before it is likely to see widespread use on mission-critical devices in the IACS environment. At the time of publication, it was only sporadically deployed on noncritical workstations on a case-by-case basis.

### 6.3.6 Future directions

Future directions include the following:

- improved central administration and management of distributed host-based firewalls;
- dynamic modification of local firewall policy based on system-wide events;
- using host-based firewalls for distributed intrusion detection.

### 6.3.7 Recommendations and guidance

There are relatively few host-based firewalls in the IACS environment. In general, control systems will not permit the use of firewalls or similar software, and vendors may prohibit this

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

type of software on their workstations. Commercially available firewalls are unaware of industrial protocols such as MODBUS/TCP® or Ethernet/IP®. Therefore, these firewalls cannot examine SCADA packets at the application layer or offer proxy services for these protocols. At the time of publication, no commercial package had been identified that offered a solution to this problem.

As seen, the development of firewalls that understand protocols and can implement rules to filter SCADA traffic is needed. In response to this need, an open-source MODBUS® has been developed that is aware of firewall extensions to the Linux® kernel. The software is available free from <http://modbusfw.sourceforge.net/>. Development of similar solutions for other platforms and configuration would facilitate widespread deployment of these new firewalls in the industry.

The development of micro-firewalls for individual use near field control devices is needed. The concept of distributed micro-firewalls for protecting critical programmable logic controls (PLCs) and RTUs has been proposed, but only limited development work has been done. The concept would be to have a micro-firewall installed in front of each individual controller or terminal to protect each from a malicious attack. These micro-firewalls would offer a second layer of defence inside the process control network (PCN) firewall and protect the system from attacks originating within the PCN. There were two promising efforts to address this problem at the time of publication. First, the British Columbia Institute of Technology had initiated a project to develop a prototype of such a system. Second, Siemens had plans to release a VPN gateway that could also act as a distributed micro-firewall.

### 6.3.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [IATF]
- [CR]
- [SANS1]
- [SSS]
- [Zur]
- [Har1]

## 6.4 Virtual Networks

### 6.4.1 Overview

Virtual Local Area Networks (VLANs) divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through configuration of Ethernet switches. Each VLAN consists of a single broadcast domain that isolates traffic from other VLANs. Just as replacing hubs with switches reduces the Ethernet® collision domain, using VLANs limits the broadcast/domain, as well as allows logical subnets to span multiple physical locations.

VLANs typically require Ethernet frame tagging using IEEE 802.1Q or proprietary standards such as inter-switch link, so that only those frames that belong to the VLAN can be transmitted to or received from ports configured on that network. Switches typically provide trunking characteristics and the exchange of VLAN database information so that updates can propagate through multiple inter-connected switches.

There are two categories of VLANs:

- Static: Often referred to as “port-based,” where switch ports are assigned to a VLAN so that it is transparent to the end user.
- Dynamic: End device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

Although more than one IP subnet may coexist on the same VLAN, the general recommendation is to use a one-to-one relationship between subnets and VLANs. This practice requires a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can be used to route between multiple logical networks.

### 6.4.2 Security vulnerabilities addressed by this technology

VLANs are not typically deployed to address host or network vulnerabilities in the same way that firewalls or intrusion detection systems are. However, when properly configured, VLANs do allow switches to enforce security policies and segregate traffic at the Ethernet layer. Properly segmented networks can also mitigate the risks of broadcast storms that may result from port scanning or worm activity.

### 6.4.3 Known issues and weaknesses

Switches have been susceptible to attacks such as media access control (MAC) spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. VLAN hopping (the ability for an attack to inject frames to unauthorized ports) has been demonstrated using switch spoofing or double-encapsulated frames. These attacks cannot be conducted remotely and require local physical access to the switch. A variety of features such as MAC address filtering, port-based authentication using IEEE 802.1x, and specific vendor best practices can be used to mitigate these attacks against the VLAN, depending on the device and implementation.

### 6.4.4 Assessment of use in the industrial automation and control systems environment

Field area networks (FANs), which are also called fieldbus systems, are ideally suited for use in the IACS environment. In general, FANs can cover larger distances than local area networks (LANs). Also, FANs have low data rates and, since FANs transport mainly process data, the size of data packets is small while real-time capabilities are important. On the other hand, LANs have high data rates and carry large amounts of data in large packets. For LANs, timeliness is not a primary concern and real-time behaviour is not required. LANs are not as well suited for use in industrial automation and control systems environment.

VLANs have been effectively deployed in plant floor networks with each automation cell, even those containing FANs, assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches.

### 6.4.5 Future directions

Although routers have provided support for IEEE 802.1Q frame tagging, firewall support for tagged packets and virtual interfaces has only recently been released. When combined with port-based authentication (802.1x), it may be possible to assign control system users to trusted (or less trusted) VLANs based on authentication credentials or the integrity of the operating system.

### 6.4.6 Recommendations and guidance

Adherence to vendor best practices can assist in ensuring secure VLAN deployment. However, there is widespread, strong interest in using the Internet in new and various ways with the control systems to increase productivity and seamless connectivity between the control system and the industrial enterprise. Along these lines, connecting FANs to the Internet is the next widely encompassing step in industrial automation and control systems. This connection could be done via a VPN type tunnelling approach or through gateways, based on either Web technologies or higher level protocols. Web technologies include Hypertext Transfer Protocol (http), Java®, and Extensible Markup Language. Higher level protocols include SNMP and Lightweight Directory Access Protocol (LDAP).

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 6.4.7 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Intel]
- [UCD]
- [802.1Q]
- [Cisco]
- [Zur]
- [Har1]

## 7 Encryption technologies and data validation

### 7.1 General

Encryption is the process of encoding and decoding data in order to ensure that information is accessible only to those authorized to have access. Data validation technologies safeguard the accuracy and completeness of information used in the industrial process.

### 7.2 Symmetric (secret) key encryption

#### 7.2.1 Overview

Symmetric (or secret) key encryption involves transforming a digital message (called the plaintext) into an apparently uncorrelated bit stream known as the ciphertext. A well-defined algorithm that has two inputs performs the reversible transformation:

- the plaintext (for encryption) or ciphertext (for decryption);
- a secret bit string known as the key.

A receiving device in possession of the same algorithm and key can transform the ciphertext back into the original plaintext message. Without the key, the inverse transformation is computationally infeasible. The name “symmetric encryption” is due to the fact that the same key and reversible algorithm are used both to encrypt the original plaintext message and to decrypt the ciphertext message.

A simple analogy is the combination lock whose mechanism is knowable from the package literature or by studying a lock that has been disassembled. The combination (often a set of 3 numbers between 0 and 35) is the “key” for the lock. It is easy to open the lock when the key is known. Trying all possible combinations will eventually open the lock, so these locks are only adequate if the cost of trying on average half of the possible physically distinct combinations ($0{,}5 \times 36^3$) is greater than the value of whatever the lock protects. Locks with a greater set of numbers in the combination provide greater protection.

Similarly, larger symmetric keys generally provide greater protection. Cryptographic systems are considered secure when the effort required to recover the key or the protected message costs more than the value imparted by that recovery.

Effective encryption requires that both the sender and the intended recipient have the same key and keep it secret from others. The security of the cryptographic system rests on the difficulty of determining the correct key rather than on a secret algorithm. Unclassified symmetric key algorithms are published and extensively cryptanalyzed before they are considered suitable for use. The list approved by the U.S. National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) 140-2 includes Triple Digital Encryption Standard (3DES) and the Advanced Encryption Standard (AES). AES is often designated as AES-128, AES-192, or AES-256, to indicate the number of bits in the key. The older Digital Encryption Standard is being phased out.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

The algorithms described above are all “block” ciphers because they encrypt in blocks, frequently padding the end of the message to make it a multiple of the block length before encryption. Changing one bit of a ciphertext block randomly alters 50 % of the resulting block of plaintext after decryption. A block cipher typically is used as a building block to create a stream cipher in what is known as a “mode of operation.” The two most employed stream cipher modes of block ciphers are:

- Counter mode (for message confidentiality), where a composite value consisting of a message count and block-within-message count are encrypted to provide a unique “keystream” block that is then combined reversibly with the plaintext block to create ciphertext, and vice versa.
- Cipher block-chaining mode (for message integrity), where a cascade of block encryptions of plaintext, each combined with the prior cumulative encryption, provides a cryptographic checksum of the entire message.

Conceptually, a stream cipher encrypts and decrypts information in units of a single bit. Native stream ciphers typically feed back the plaintext of the message, in some form, to modify the key of the cipher throughout the encryption of decryption operation, in a process generically known as autokey. This is in contrast to stream cipher modes of block ciphers, which typically use a single unmodified key for each successive encryption and decryption operation. Native stream ciphers have long been used by governments to protect their classified communications, but have received little attention from the open research community. There are no NIST-approved native stream ciphers.

### 7.2.2 Security vulnerabilities addressed by this technology

Symmetric key encryption is most effective when used as a building block to provide data confidentiality (privacy), so that anyone “listening” to the data cannot understand it, and as an essential component of message integrity and message source authentication. When used in a link encryptor (explained under 7.2.3), symmetric key encryption can be used to distinguish communication by devices that are not part of the desired network. This feature is generally attractive for SCADA and other process control systems that wish to allow little or no access to the control network, but is difficult to deploy in systems requiring unrestricted Internet access. Refer to public key encryption and key distribution for details on addressing other vulnerabilities, such as authentication and key distribution risks.

### 7.2.3 Typical deployment

Symmetric key cryptography is typically implemented as either a link encryptor or embedded in the device to be protected. Each method is explained below.

a) Link encryptors: A link encryptor is a hardware unit with two or more distinct data ports. One or more ports are called the plaintext (or red) ports; these receive data to be encrypted when the attached equipment is transmitting and send decrypted data when the attached equipment is receiving. The remaining port is the ciphertext (or black) port; it sends the encrypted data stream (and often other protocol information) to the ciphertext port of one or more units and receives ciphertext information from those units. Within a link encryptor, plaintext and ciphertext ports need to be separate.

   The receiving link encryptor accepts, decrypts, and passes the data to the receiving attached equipment. Some link encryptors provide an additional dedicated port for management functions, such as initialization, maintenance, and key change. Link encryptors are often used to retrofit equipment that is already installed on a network and has limited physical access.

b) Embedded cryptography: Symmetric key cryptography may also be embedded in a cryptographic module inside the unit to be protected, often on a special purpose chip. In principle, cryptographic routines could be incorporated into the programs in process control equipment. However, special purpose processors often can do extensive mathematics more quickly, and keeping cryptographic portions separate may make them more secure. Embedded cryptography is often the preferred deployment, but is often not practical to retrofit in existing control or SCADA systems.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 7.2.4 Known issues and weaknesses

Modern cryptographic algorithms are rarely broken by direct attack. Most failures are due to poor protocol, inside information, poor security policy, or deception attacks on the human component of the system. Even with good algorithms, cryptographic systems with inadequate protocols may be attacked by recording and replaying messages, studying message patterns, message forgery or alteration, or key loss/theft.

Communication noise can be a problem because good cryptographic algorithms alter a message unpredictably, even if only a single bit is changed. Cryptography also slows communications because additional time is required to encrypt, decrypt, and authenticate the message. In addition, encrypted messages are often longer than unencrypted messages due to one or more of the following items:

- additional check sums to reduce errors;
- protocols to control the cryptography;
- padding (for block ciphers);
- authentication procedures;
- other required cryptographic processes.

Time increases can be in the tens of milliseconds for retrofit link encryptors on slow lines (300 Bd to 19 600 Bd) and milliseconds for embedded encryption.

Depending on the protocol and system configuration, there may be problems with link encryptors encrypting both the message and the address, making messages impossible to route in a multi-drop configuration. Some systems may not support broadcast or multicast commands.

Cryptography also introduces key management issues. Good security policies require periodic key changes. This process becomes more difficult as the geographic size of the process control system increases, with extensive SCADA systems being the most severe example. Because site visits to change keys can be costly and slow, it is useful to be able to change keys remotely. Key management issues are described more fully under public key cryptography (see 7.3).

The most effective safeguard is to use a complete cryptographic system approved by an accredited cryptographic certification laboratory. The NIST/CSE Cryptographic Module Validation Program (CMVP) is the best known and is internationally recognized. Even then, the technology is only effective if it is an integral part of an effectively enforced information security policy. American Gas Association (AGA) report 12-1 (see [AGA 12]) contains an example of such a security policy. While it is directed toward a SCADA system, much of its policy recommendations could apply to any manufacturing or control system.

### 7.2.5 Assessment of use in the industrial automation and control systems environment

Cryptography does not appear to be in widespread use in IACSs at the current time. Process control data passing between devices on the IACS network may not need to be encrypted due to the reduced vulnerability of the data within a physically secure area. However, when data passes over wide area networks or the Internet to off-site users or support personnel, then communications should be encrypted to protect both the confidentially and the integrity of the data. In instances where process control data passes between the IACS network and the site LAN, the relative vulnerability and criticality shall be assessed to determine whether cryptography is appropriate.

### 7.2.6 Future directions

A variety of proprietary cryptographic systems will probably enter the marketplace in the near future. It is also likely that products will appear that claim to use widely recognized algorithms

IECNORM.COM : Click to view the full PDF of IEC/TR 62443 3-1 ed 1.0:2009

(such as AES, 3DES, etc.) with proprietary protocols. Several standards and government organizations will make recommendations and compliant products will emerge. Both retrofit and embedded products that comply with AGA 12-1 (see [AGA-12]) will continue to enter the market in the coming years.

### 7.2.7 Recommendations and guidance

Overall, cryptography shall be deployed as part of a comprehensive, enforced security policy. Select cryptographic protection matched to the value of the information and control system assets being protected and IACS operating constraints. Specifically, the cryptographic key should be long enough that guessing it takes more effort, time, and cost than the value of the protected asset.

Also, protect encryption hardware from physical tampering and uncontrolled electronic connections. Select cryptographic protection with remote key management if the units being protected are so numerous or geographically dispersed that changing keys is difficult or expensive. Additionally, consider the following when protecting highly valuable control system data and information through cryptography.

a) Require separate plaintext and ciphertext ports unless the network absolutely requires the restriction to pass both plaintext and ciphertext through each port.

b) Use only units that can be certified to comply with a standard, such as FIPS 140-2 (see [NIST11] through the CMVP. Standards ensure that cryptographic systems were studied carefully for weaknesses by a wide range of experts, rather than being developed by a few engineers in a single company. At a minimum, certification makes it probable that:

- some method (such as counter mode) will be used to ensure that the same message does not generate the same value each time;
- IACS messages are protected against replay and forging;
- key management is secure throughout the life cycle of the key;
- the system is using a good quality random number generator;
- the entire system has been implemented securely.

The AGA12-2 report provides a good example of an industry consensus approach. While it is directed toward gas industry SCADA systems, it has many characteristics that apply to any IACS.

### 7.2.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [NIST01], [NIST03], [NIST06], [NIST07], [NIST07A], [NIST07B], [NIST11]
- [AGA-12-1]
- [MvOV]
- [Sch]
- [Smi]
- [AGA-12]
- [NIST10]
- [IAONA]
- [KP], pp. 50-55
- [anon03], [anon07], [anon08], [anon37], [anon41]
- [ST]
- [Pet1]
- [Lam]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1:2009

- [GP]
- [Coh]
- [Zur]
- [Har1]
- [Sch], pp. 3, 5, 39
- [Teu], p. 92

### 7.3 Public key encryption and key distribution

#### 7.3.1 Overview

As noted in 7.2, secret key cryptography uses a single key in a symmetric manner for both encryption and decryption. In public key cryptography, a pair of different but related keys, usually known as a public-private key pair, replaces that single key. The private and public keys are mathematically related such that a public key can be used by others to encrypt messages to be sent to the holder of the corresponding private key, which then can be decrypted with that private key. Similarly, a private key can be used to sign a cryptographic hash of a document, after which others can validate the signature via the corresponding public key. A key holder usually circulates the public key to other users in the same community, but does not reveal the corresponding private key to the other users.

The security of the system rests on the secrecy of the private key. The public and private key pair may be generated directly by the user, or may be received by the user from some central key generation authority. This latter approach is particularly appropriate when there are legal or corporate key escrow requirements, since such requirements generally obligate the key generator to escrow the key(s) before their use.

To minimize requirements for legal or corporate key escrow, and to enhance the protection of authentication (and signing) keys, in some applications it is recommended that separate key pairs be used for encryption and authentication. Only the encryption private key needs to be backed up in such cases. This allows the private authentication key to be generated and retained at all times by the user, thus enhancing security. This is the default mode of operation for some key management systems. Recovery from the loss of the private authentication key is provided by the issue of a new key pair. Since data is not encrypted with the authentication key pair, no data is lost.

#### 7.3.2 Security vulnerabilities addressed by this technology

Shared secrets used in symmetric encryption schemes leave open the possibility of one of the participants being compromised, thus compromising all portions of the system that rely on the secret being secure. Further, some mechanism shall be provided for the sender(s) and receiver(s) to share the secret. If the secret cannot be shared securely, then there is no point to having a shared secret. Since password hashes typically use one-way hashing algorithms with known vulnerabilities, simple username and password authentication mechanisms are vulnerable to anyone with knowledge of the algorithm used. Therefore, other, more robust means of sharing the secrets are required.

Public (asymmetric) key cryptography addresses the weaknesses of shared secrets and one-way hashing algorithms by providing a framework wherein the latter can show their true value.

Fast encryption of arbitrary data is best done using symmetric key algorithms. The problem with such algorithms is their need to securely share a common secret key. Using asymmetric cryptography, a sender encrypts a sharable secret (the symmetric encryption key) using the intended recipient's public key, then passes it to the recipient. The recipient decrypts this now-shared secret using its private key. At this point, both recipient and sender have a shared secret that they can use to encrypt arbitrary data at a very high rate of speed. The same technique can work for multiple recipients sharing a single key; each receives the same secret encrypted under its own public key, and decrypts that information with its private key to retrieve

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

the shared secret. For example, the S/MIME secure email standard implemented in most modern email programs uses this approach, with each message containing a separate public-key-encrypted version of the message key for each intended recipient; the message content is encrypted using this symmetric key.

When an additional layer of authentication is provided (e.g., through a public key infrastructure-PKI or a trusted certificate authority server), the public keys of the recipient(s) can be authenticated via the trusted third party before setting up a secure channel for data communication.

Public key cryptography also provides the potential for unforgeable digital signatures. Information to be signed, such as a contract or data record, is compressed via a cryptographic one-way function (a hash) into a short bit string. A private key is used to transform that short bit string, which anyone can compute, into an equivalent string dependent on the private key. Anyone wishing to validate the digital signature can compute his own cryptographic hash of the original digital document and compare it to the string he gets when he applies the corresponding public key to the purported signature. If the two compare, the holder of the private key signed the digital document or record.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1:2009

### 7.3.3 Typical deployment

Public key authentication is most commonly deployed in the following applications:

- transport-layer-security (IETF TLS or Secure Sockets Layer-IETF SSL);
- virtual public network technologies, such as Internet Protocol Security (IPsec);
- Secure-Shell (IETF SSH);
- Kerberos (three-way-handshake) authentication using a certificate authority.

### 7.3.4 Known issues and weaknesses

There are no known security weaknesses with the dominant public key/PKI encryption algorithms. However, the security these algorithms provide depends on key length, the quality of the key generation and key management, and how users implement and use PKI. Users need to understand how to properly create, distribute, and protect their keys. The greatest weakness comes from users who do not use the technology properly.

The most significant weakness to any public-key based system is what is known as a “man-in-the-middle” attack. If a perpetrator is successful at inserting himself between a sender and a receiver, the perpetrator can pretend to be the recipient to the sender, and pretend to be the sender to the recipient, through use of the perpetrator’s own public-private key pair. The best way to protect against this vulnerability is to use a public key infrastructure or equivalent to issue signed certificates authenticating all public keys used. Time limits should also be put on the use of keys. Public key infrastructures conforming to modern standards such as PKIX (RFC 3280) and suitable protection profiles address many of these concerns. The Kerberos authentication rubric developed at Massachusetts Institute of Technology (MIT) is able to address weakness and is available on most OS platforms.

The processing required for some public key algorithms is very central processing unit (CPU) intensive and cannot be reasonably supported on many 16-bit or smaller CPUs. Nor can it meet the demands of sub-second time-critical communications, even on very fast CPUs. Its primary use is in distributing session keys for symmetric (secret) key encryption of the messaging within a session, and for digitally signing documents and validating signed documents.

### 7.3.5 Assessment of use in the industrial automation and control systems environment

Public (asymmetric) key encryption provides a generic means of solving the issues of key distribution and unforgeable digital signatures. However, initially deployed public key algorithms

are much slower than most symmetric key encryption algorithms and the keys shall be very long. For example, a 1024-bit Rivest, Shamir and Adleman (RSA®) public key is roughly equivalent to an 80-bit symmetric key. Newer public key algorithms address these issues. An elliptical curve (EC) public key equivalent to an 80-bit symmetric key is only 160 bits. The heavy computational requirements and, for small systems, the required extra memory are the primary hurdles to deployment of asymmetric encryption in the IACS environment.

A general constraint with using encryption in an IACS environment is the limitation due to time-critical performance, including HMI response time. With rare exception, data and message encryption in such systems should use symmetric key algorithms, the keys for which have previously been shared using asymmetric (public) key encryption techniques. That sharing usually shall be done without time-critical constraints.

The heavy performance burden of public key cryptography generally prohibits time-critical use of digital signatures, at least with low-computer-power devices. However, when authentication and non-repudiation (undeniability) are more important than performance, digital signatures provide an appropriate tool.

### 7.3.6 Future directions

In the past, SCADA monitoring and control system communication were somewhat secure because these systems were developed without cyber connections to the outside world. As outside cyber connections are made to these systems, they have become quite vulnerable. In the future, public key cryptography should play a significant role in the securing of SCADA and other control systems.

Public key algorithms are continuing to evolve in order to provide better security for cyber systems to counteract attackers that are continually obtaining more sophisticated methodologies and tools. Currently, the best-known public key algorithm is RSA®. RSA® is named after its inventors at MIT, Rivest, Shamir, and Adleman. RSA® is a block cipher that is popular although its key length has been increased over recent years. Additional key length puts a heavier processing load on applications. Unfortunately, additional key length slows the communication process down often to unacceptable levels for application in IACS.

A competitive approach that promises similar security as RSA®, while using far smaller key lengths, is elliptic curve cryptosystem (ECC). With the acceptance of ECC methods by U.S. NIST, it is expected that more systems will become available using these more efficient algorithms.

### 7.3.7 Problems of encryption usage

Additional security is warranted for SCADA and other IACSs as these systems become connected to the outside world. Consequently, as these systems become connected, attackers may gain access through the use of the Internet and other pathways. Symmetric (secret) key encryption, discussed in 7.2, is a good method to secure IACSs. On the other hand, the current state-of-the-art public key encryption does not lend public key encryption to be viable for IACSs because the process itself is very slow and has its own problems. Symmetric key systems are usually much faster than their public key counterparts. Public key systems do have their place in the securing of IACSs. Public key systems may be used for exchanging the secret key for use in later communications through symmetric key systems. This hybrid approach is a common design that benefits from both the high speed of symmetric key systems and a secure key exchange using public key systems.

A problem with public key systems is the authenticity of the public key. An attacker may offer the sender his own public key and pretend that it originates from the legitimate receiver. The sender then uses the fake public key to perform his encryption, and the attacker can simply decrypt the message using his private key. In order to thwart an attacker that attempts to substitute his public key for the victim's key, certificates are used. A certificate combines user information with the user's public key and is signed by a trusted authority that guarantees the key belongs to the user. The trusted authority is usually called a certification authority, a

IECNORM.COM : Click to view the full PDF of IEC TR 62443-3-1:2009

component of a PKI. The certificate of a certification authority itself is usually verified by a higher level certification authority that confirms that the certification authority's certificate is genuine and contains its public key.

### 7.3.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [anon30], [anon32], [anon38], [anon40]
- [Man]
- [Zur]
- [Har1]

## 7.4 Virtual private networks (VPNs)

### 7.4.1 Overview

One method of encrypting data is through a VPN. A VPN is a private network that operates as an overlay on a public infrastructure. It contains three components, which are handled at the recipient end of the VPN:

- Authenticity and authentication: Security measures designed to establish the validity of a transmission, message, originator, or a means of verifying an individual's authorization to receive specific categories of information [INFOSEC-99][4];
- Integrity: In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information [INFOSEC-99][5];
- Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices [INFOSEC-99][6].

A secondary component of VPNs is authorization, which encompasses:

- The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs;
- Access privileges granted to a user, program, or process [INFOSEC-99] [7].

Other classes of technology, such as multi-protocol label switching, frame relay and asynchronous transfer mode, may be referred to misleadingly as VPNs because they enable a private network to work over a public infrastructure. However, these technologies do not natively contain all the primary components of a VPN as described above.

### 7.4.2 Security vulnerabilities addressed by this technology

A VPN is intended to allow a private network to function across a public network. A VPN can provide the same type of security on a network as an armoured car can for securely transporting company information or material between physical premises. It protects information in transport from the “outside" world. For the IACS environment, the outside world typically includes corporate LAN users who are not authorized to operate control centre equipment. The VPN can provide the following services:

- Control access into a trusted network via authentication;
- Maintain the integrity of the trusted data on an untrusted network;

IECNORM.COM : Click to view the full PDF of IEC TR 62443-3-1 ed 1.0:2009

4 <http://www.atis.org/tg2k/_authentication.html>

5 <http://www.atis.org/tg2k/_integrity.html>

6 <http://www.atis.org/tg2k/_confidentiality.html>

7 <http://www.atis.org/tg2k/_authorization.html>

- Record information useful for traffic monitoring, analysis and intrusion detection.

### 7.4.3 Typical deployment

In general, there are three classifications of VPN deployments that use security gateways and hosts to create VPN connectivity.

- A security gateway is an intermediate system that uses VPN technology to secure traffic that transverses a pair of security gateways. Security gateways are also commonly used to implement authorization for the traffic that traverses the device. Security gateway functionality has been implemented in existing internetworking devices such as firewalls, routers, and switches. New terms, such as VPN Concentrator and VPN Gateway, were created for dedicated computing devices that terminate large amounts of VPN traffic.
- The host uses VPN technology to secure traffic that originates or is destined for the host. The VPN technology used by the host is either included in the host's native operating system or added to the host operating system specifically to enable VPN access.

The three classifications of VPN deployments are described in detail below.

- Security gateway to security gateway (Figure 2): The two endpoints of the VPN are intermediary devices that pass traffic from a trusted network to another trusted network, while relying on VPN technology to secure the traffic on the untrusted transport network. This type of VPN is commonly called site-to-site or LAN-to-LAN VPN.

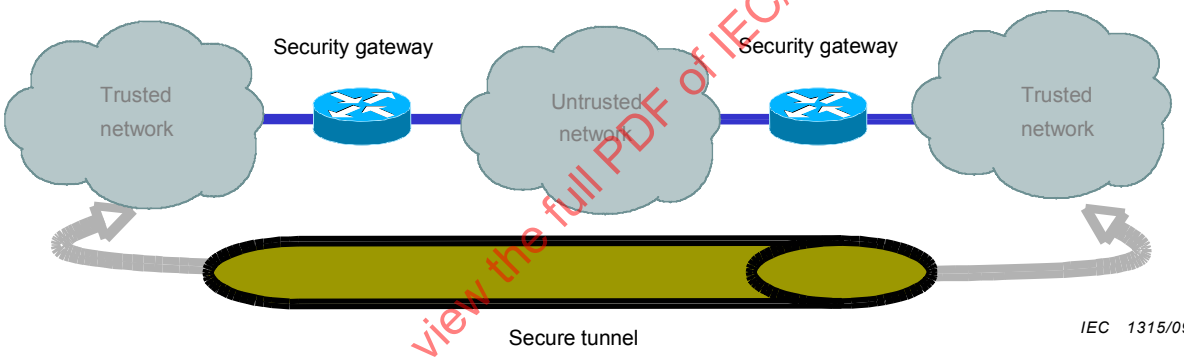


**Figure 2 – Security gateway to security gateway VPN**

- Host to security gateway (Figure 3): One endpoint is a host-computing device and the other is an intermediate device that passes traffic from the host to the trusted network behind the security gateway while relying on VPN technology to secure the traffic on the untrusted network. This type of VPN is commonly called a remote access VPN.

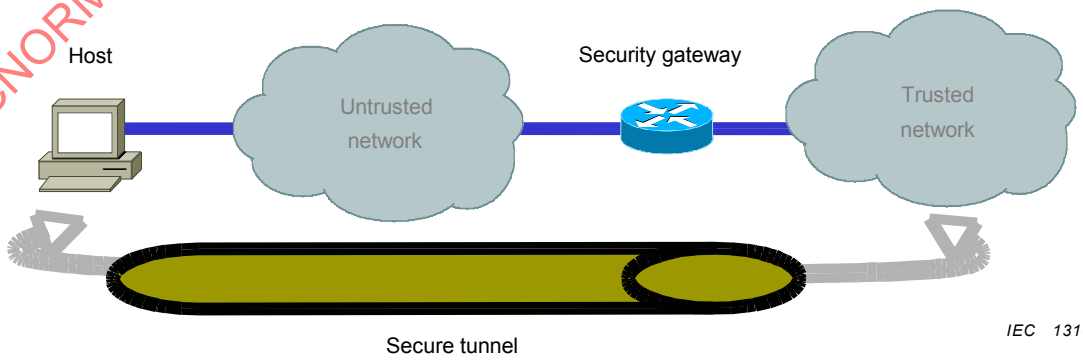


**Figure 3 – Host to security gateway VPN**

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- Host to host (Figure 4) : Each endpoint of the VPN tunnel is a host-computing device. The host devices leverage VPN technology on the host for securing the communications on the untrusted network.

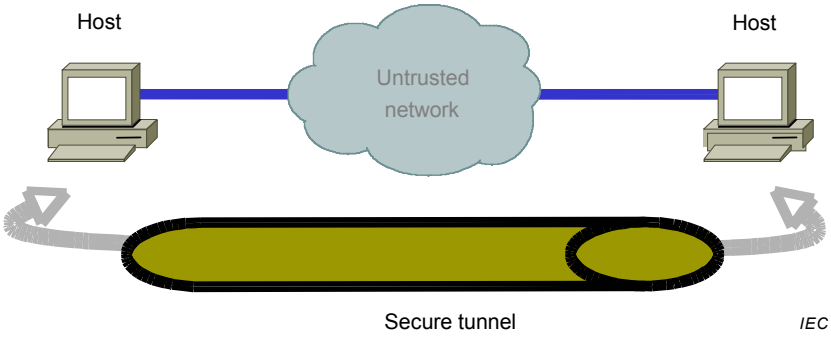


**Figure 4 – Host to host gateway VPN**

The most common types of VPN technology implemented today are the following:

- Internet protocol security (IPsec): IPsec is a set of standards defined by IETF to govern the secure communications of data across public networks and secure all IP unicast-capable applications. According to the standard, multicast applications cannot use IPsec. However, there is an IETF working group specifically looking at securing multicast traffic with IPsec. Alternatively, multicast and non-IP-based protocols can be transported through IPsec VPNs by encapsulating these protocols in an IP unicast-capable protocol and replicating the transmission to each desired VPN receiving device. For example, multicast traffic can be passed from router to router by encapsulating it in an appropriate header before being encrypted and transported via IPsec.

  IPsec is a tool included in many current operating systems. The intent of the standard is to guarantee interoperability across vendor platforms. While there are standards for vendor interoperability, the reality is that determination of interoperability of multi-vendor implementations depends on specific implementation testing conducted by the end-user organization. The protocol has been continually enhanced to address specific requirements from the market, such as extensions to the protocol to address individual user authentication and network address translation (NAT) device transversal. These extensions are typically vendor specific and can lead to interoperability issues primarily in host-to-security gateway environments.

- Secure sockets layer (SSL): SSL provides a secure channel between two machines; the channel is oblivious to the data passing through it. The IETF made slight modifications to the SSL version 3 protocol and created a new protocol called Transport Layer Security (TLS). SSL and TLS are often used interchangeably. This report generically uses the SSL terminology.

  SSL is most often recognized for securing HTTP traffic. This protocol implementation is known as HTTP Secure (HTTPS). However, SSL is not limited to securing just HTTP traffic; it can be used to secure many different application layer programs. SSL-based VPN products have gained acceptance because of the market for “clientless” VPN products. The clientless terminology is deemed appropriate for most network operating systems because they include SSL implementation in the operating systems embedded web browser. The VPN administrator does not have to install third-party VPN “client” software, and can create a “clientless” VPN. The real benefit is not that the implementation is clientless, but that client installation requires little or no administration.

- Secure shell (SSH): SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Web and other types of servers. The latest version, SSH2, is a proposed set of standards from the IETF[8]. Typically, SSH is deployed as a secure alternative to the telnet application.

8 <http://whatis.techtarget.com/definition/0,289893,sid9_gci214091,00.html>

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

However, SSH also has the ability to do port forwarding, which allows it to be used in all three deployments listed above. SSH is included in the majority of UNIX® distributions on the market, and is typically added to other platforms through a third-party package.

It is possible to overlay VPN technologies on each other in order to provide secure access to and through security perimeters. For instance, a company may deploy an IPsec VPN to provide secure access to the company's edge perimeter. The company may then deploy an SSL VPN server to allow particular users to gain access to a security perimeter embedded within the company.

### 7.4.4 Known issues and weaknesses

VPNs do not protect a network and workstations against most data-driven attacks (i.e., viruses), some denial-of-service attacks, social engineering attacks, and malicious insiders.

Depending on the VPN technology chosen, the primary challenges for VPNs have been:

- Interoperability: This issue is primarily associated with IPsec due to different interpretations of the IPsec RFCs, and is typically mitigated within a company by selecting a standard IPsec VPN client and termination devices from a particular vendor.
- Setup: As mentioned above, there are several initiatives in the market to make setting up VPNs easier by either introducing new technologies or increasing the ease of use of the existing technologies.
- Ongoing support and maintenance: Because VPNs are a technology overlay to an existing network, companies have to spend operational resources to maintain the overlay and change it when the underlying infrastructure changes.

Each VPN technology has its trade-offs. For example, SSL-based VPNs are viewed as being easier to configure than IPsec VPNs on the client, but they do not support the wide variety of applications and protocols that IPsec VPNs do.

### 7.4.5 Assessment of use in the industrial automation and control systems environment

VPNs are most often used in the IACS environment to provide secure access from an untrusted network to the PCN. Untrusted networks can range from the Internet to the corporate LAN. Properly configured, VPNs can greatly restrict access to and from control system host computers and controllers and therefore improve security. They can also potentially improve PCN responsiveness by removing unauthorized non-essential traffic from the intermediary network.

Other possible deployments include using either host-based or mini-standalone security gateways, either interposed before or running on individual control devices. This technique of implementing VPNs on an individual device basis can have significant administration overhead.

Additional issues of using VPNs in the IACS environment include:

- The lack of VPN products available for non-IP based protocols such as Foundation Fieldbus®, PROFIBUS®, or any serial-based network. Emerging approaches such as AGA-12 are being developed for some legacy communications protocols.
- The lack of host-based (software) VPN products available for typical controller-based operating systems found in PLCs, RTUs, and DCSs.
- The potential incompatibility between host-based (software) VPN products and Windows® or UNIX® control system software.
- The addition of latency to control system communications. This issue requires further research and testing.
- VPN reconnect times may be too long to use on mission critical links. This issue requires further research and testing.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- The lack of support in transport layer encryption schemes for IACS protocols such as PROFInet®, Ethernet/IP®, Foundation Fieldbus HSE®, or Modbus/TCP®.
- The lack of experience in designing large-scale VPNs for industrial applications.
- The overhead required to manage VPNs in widely dispersed systems typical of SCADA environments.

#### 7.4.6 Future directions

Future directions include embedded VPN technologies in the network and end devices.

#### 7.4.7 Recommendations and guidance

VPN devices used to protect control systems should be thoroughly tested to verify that the VPN technology is compatible with the application and that the VPN devices do not unacceptably affect traffic characteristics of the implementation.

#### 7.4.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Smi]
- [Res]

## 8 Management, audit, measurement, monitoring, and detection tools

### 8.1 General

Audit, monitoring, and detection tools provide the ability to analyze security vulnerabilities, detect possible compromises, and forensically analyze compromise incidents. These technologies include virus detection systems, intrusion detection systems, host logging/auditing utilities, event correlation engines, and network forensics tools.

### 8.2 Log auditing utilities

#### 8.2.1 Overview

Security incidents leave traces. The number of traces and the various files and entries created by an attack can offer valuable information about the extent of the attack, which areas of a system are affected, and even when an attack is currently in progress.

Typically, each server is responsible for maintaining a set of systems logs individually. When the size and complexity of a network go up, so does the number of logs which might record a hostile act. Unfortunately, so too does the time it takes a system administrator to manage the logs.

Any security policy shall plan for the regular auditing and maintenance of critical logs and system trace files for the likelihood of catching and being able to repair damage from an attack.

For example, administrators typically monitor the success and failure of logon events, changes to local accounts, and changes to local security policy. Although logon success events can help reconstruct a specific user's activities, administrators look primarily for events that document a consistent pattern of failed logons or failed attempts to change the local security policy.

Most operating systems have an extensive set of logs and utilities for maintaining log files. For example, Microsoft Windows® 2000 has two utilities delivered with the Advanced Server 2000 Resource Kit:

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

AuditPol—AuditPol can be used to display current security audit settings, to enable or disable security auditing, and to adjust the audit criteria for nine categories of security events.

Dumpel—Dumpel, a command-line tool, can be used to extract events from the system, security, or application log on a local or remote system.

The system registry is also an attack target. With the advent of the security configuration tools with group policy and the ability to centrally distribute registry security changes to hundreds or thousands of workstations, security issues are likely to become more commonplace as organizations seek to enhance system security at all levels.

Fortunately there are many tools and utilities to help here. Some can be found in the Resource Kit for the Windows® 2000 advanced server. These tools are of the kinds that manage backups, restoration of local and remote system registries and kernel settings. On Microsoft platforms, tools such as WinDiff can be scripted to examine the differences between daily backups of registries to ascertain if any unforeseen or unregulated change has taken place.

### 8.2.2 Security vulnerabilities addressed by this technology

Using a security-auditing tool such as AuditPol, administrators can check the numbers, types and responses to authentication attempts on a network over one or more systems. The kinds of events such tools as AuditPol can monitor are the following:

- Account events (account logon events) monitor logon attempts on a domain controller (DC);
- Directory (directory service access) is a generic category that can be enabled to audit access to DC objects;
- Logon events (logon events) monitor logon attempts on the local system;
- Object access (object access) is a generic category that can be enabled to track access to a specific file, folder, or shared resource;
- Policy events (policy change) track changes to the local security policy;
- Privilege events (privilege use) monitor operations that grant elevated privileges to user or group accounts;
- Process (process tracking) is a generic category that can be enabled to audit access to a specific process;
- Security Account Manager (SAM) events (account management) monitor changes to individual or group accounts on the local system in the SAM database;
- System events (system events) include system and service startup and shutdown, messages from the browser, routing and remote access service, or the Win32 time service.

In the case of Dumpel, logs from one or more systems may be screened, backed up and parsed out for key security events such as password/authentication lockout, access using guest or administration accounts and so on.

Such tools as Windiff can parse and examine the differences between chronological logs or logs taken from identically configured machines to derive if any unscheduled or unregulated change has been done.

Also the Windows® Resource Kits includes the following utilities:

- System Difference Packages (SysDiff) is a Resource Kit utility that allows users to quickly take before-and-after snapshots of their file system and registry. Using the difference information, Sysdiff builds a binary package that can be used to install the changes made by the snapshot. Sysdiff is typically used to install applications using a snapshot method. However, for this discussion, users can log Sysdiff changes and then view them in readable text form, which lets them view the Registry changes made by a particular application.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed. 1.0:2009

- Installer is a utility found in the Resource Kit that serves as another useful tool for monitoring the changes made during an application installation. This often-overlooked utility can be very useful because it monitors all activity around an application installation, including the API calls the setup program uses to modify the registry.

And in available freeware:

RegMon is a most useful registry troubleshooting tool. It allows users to spy on registry activity created by a given process. RegMon comprises an executable (regmon.exe) and a kernel-mode filter driver (regsys.sys) that installs by default when RegMon is first launched.

### 8.2.3 Typical deployment

For the Microsoft 2000 utilities, the tools are deployed to manage one or more remote servers and typically support an extensive scripting and command line interface. The Microsoft tools also fit into the Microsoft Management Console as a snap in.

The most effective use of these tools is to have them triggered on events that are of interest or to have a regular backup and screening of event files. RegMon is a tool that can spy on processes that make changes to the registry.

### 8.2.4 Known issues and weaknesses

Most of the system administrator tools that may be used in a log auditing policy require extensive scripting and management. This is a problem in rapidly changing network environments or in wireless fidelity (Wi-Fi) situations where machines are entering and leaving the network domains regularly.

The scripts need to be extensively documented and maintained; otherwise, they will quickly become obsolete and ineffective. The alternative is to have a lower level of auditing based on the easily configured or default settings of the tools, or by relying on common standards of setup and management of the network environment. Both of these methods impose a load on a system administrator.

### 8.2.5 Assessment of use in the industrial automation and control systems environment

In an IACS environment, use of these tools requires the extensive knowledge of an IT professional in this area of computing technology with critical production and safety implications for the facility.

These networks are typically very stable in configuration and as such will lend themselves well to the use of managed scripts for auditing and maintenance.

The critical tasks in network management in an IACS environment are security and authentication management, registry and installation integrity management, and all those functions that can augment an installation and operational qualification exercise in the regulated manufacturing environments. The judicious use of auditing and log management tools can provide valuable assistance in maintaining and proving the integrity of an IACS system from installation through the system lifecycle. The value of such tools in this environment can be calculated by the effort required to requalify or otherwise retest an IACS system where the integrity due to attack, or due to accident or error, is in question.

### 8.2.6 Future directions

In the future, auditing utilities may use web servers for auditing and management, as well as Wi-Fi and highly flexible network configurations.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 8.2.7 Recommendations and guidance

Use of system auditing utilities should be planned at the inception of an IACS project or retrofitted as soon as is convenient. There is enough value in providing a tangible log of evidence of the integrity of a system to warrant their use. Additionally, active log management utilities can actually flag an attack or event in progress and provide location and tracing information to help respond to an attack.

### 8.2.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [SANS3]
- [M-E]
- [Seq]
- [Sha]

## 8.3 Virus and malicious code detection systems

There is an ongoing battle between the creators of computer viruses and malicious code and the firms creating software to prevent their actions. While antivirus firms are adding proactive technology to their software, when it comes to new types of viruses, they still largely depend on reacting to the actions of the virus creators. Short of dismantling one's network, there is no way to totally protect one's environment from the next new fast-spreading virus. One thing is guaranteed in the world of malicious code: by the time one reads this, the 'black hats' and 'white hats' will have taken their competition to new levels.

Over time, malicious code has entered systems by a variety of means: from boot-sector viruses entering on floppy discs, to remote procedure call attacks, to executable scripts in email messages, to newer methods, including instant messaging and spoofed certification of controls downloaded over the internet.

Code detection systems shall therefore be comprehensive enough to cover all the possible ways a file can enter a system, and flexible enough to provide defence in depth and in method to avoid common-mode failure of protection.

In many cases, the discussion surrounding the detection of virus infections centres on the activity of antivirus software. What is often overlooked is that if antivirus software can detect an infection or an infection attempt, it can usually deal with the situation effectively. A virus incident will only occur in situations where the antivirus software was not able to detect the infecting agent, at least not initially.

There are several types of indicators for possible infection. Virus detection systems (VDS) can monitor and respond to one or more of these indicators. Indicators can result directly from a specific virus payload, as a side effect of the virus payload, or as a result of the virus's attempt to spread. Indicators of virus infection include the following:

- Interface indicators: where a screen or sound generated by the virus appears on several machines at once – for example, a cartoon sound or a screen shot of a pirate jolly roger;
- System indicators: where a host's operating profile is changed, a file share becomes unsecured suddenly, or a system function becomes disabled;
- File indicators: the appearance of unknown files on a host, or changed parameters of an executable file;
- Network indicators: like network storms, email blasts or buffer flooding attempts;
- Custom indicators: designed to address specific host functions or vulnerabilities, or designed by an administration team to isolate a viral behaviour – for example, using a dummy address book to trap malicious code which propagates by email.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 8.3.1 Security vulnerabilities addressed by this technology

A VDS serves as an active agent for detection of unusual activity categorized by the indicators above. A VDS can monitor and act upon malicious code activity at either a host or a network server level, such as an email server. A VDS can provide protection by addressing the following vulnerabilities:

- presence of a known virus, worm or Trojan horse on a host or system;
- detection of a typical pathology of behaviour of a virus, worm or Trojan horse indicating an attack is underway;
- detection, isolation and safe shutdown of systems affected by a viral attack.

### 8.3.2 Typical deployment

Virus Detection Systems may be deployed in three modes.

### 8.3.3 Known issues and weaknesses

A VDS can only function when installed, running full-time and maintained current against the state of known attack methods and payload. Typically, in a few hours of a new attack, the major VDS vendors will release a patch upgrade to provide for the detection and isolation of a new attack in the ecosystem.

An administration organization that does not ensure that all installations of a VDS are up to date and consistent with the latest pathologies will be vulnerable.

A trade-off needs to be made when considering the extent and scope of a virus detection scheme. Typically, commercial packages can be configured to carry out a range of tasks, depending on the function of the host where the software is installed. For example, a typical workstation will have a configuration set up to monitor and protect:

- against boot sector viruses at start-up;
- file share virus propagation;
- Internet and email attachment viruses.

The trade off is to configure the scanning of system, application and data files with enough frequency and scope to provide optimum protection relative to the performance degradation necessary to carry out such a task.

### 8.3.4 Assessment of use in the industrial automation and control systems environment

In the IACS environment, workstations and servers are usually dedicated to certain tasks pertinent to the operation of the facility. This includes tasks such as operations procedure review, recipe and laboratory management, logging and shift reporting and so on. Additionally, mission-critical functions such as advanced control techniques, regulatory compliance and regulatory process control are now run as applications on commercial-grade machines with common commercial operating systems such as Windows® XP, and some brands of Linux®. With the propagation of open standards for integrating these systems together using techniques such as OPC, there are many more opportunities for malicious code to propagate quickly across what used to be highly proprietary systems.

Given the capabilities of the commercial tools available, the IACS administration team shall make an assessment of the trade-off between the impact of the loss of performance inevitable in the use of an active VDS, and the incremental gain in protection in implementing all the various malicious code detection options.

Upgrading the algorithms of a commercial VDS requires importing the new algorithms by Internet or detachable media. This activity may bypass practices commonly used to isolate the

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

IACS network. Therefore, deployment of VDS in an IACS situation shall then assess the mission-criticality of each system, each configuration used, and the procedures to maintain those configurations.

#### 8.3.5 Cost range

Initial costs per host for VDS range from 20USD to 80USD. In most cases, more configurable, server-side versions are available for email and Internet servers. The major commercial VDS vendors also maintain a subscription and support service, ranging from 20 USD to several 100s USD for year-on-year updates, alerts and resources for the latest malicious code attacks.

#### 8.3.6 Future directions

Future directions include heuristics, statistical and neural net technologies for VDS. Physical access to networks will become much more prevalent using Wi-Fi.

#### 8.3.7 Recommendations and guidance

VDS configurations and policies should be carefully coordinated with intrusion-detection systems such as firewalls. Each provides a level of security and flexibility in preventing the deployment of malicious code. Unauthorized intrusions should be coordinated with the VDS to provide advance notice of possible attacks. There should be careful policy construction for the configuration, maintenance and deployment of a VDS in a secure, mission-critical IACS and the management of access to such networks.

#### 8.3.8 Information sources and reference material

The reference in square brackets listed below refers to the Bibliography.

- [SANS3]

### 8.4 Intrusion detection systems (IDS)

#### 8.4.1 Overview

An intrusion is an attempt by someone to break into or misuse a computer system. Intrusion detection systems monitor either traffic patterns on the network or files in host computers, looking for signatures that indicate an intruder has or is attempting to break into a system. These systems ensure that any unusual activity such as new open ports, unusual traffic patterns, or changes to critical operating system files are brought to the attention of the appropriate security personnel.

There are traditionally two varieties of IDS:

- Network intrusion detection systems (NIDS): Systems that monitor network traffic and alarms and respond when they identify traffic patterns that they deem to be an attack.
- Host intrusion detection systems (HIDS): Software that monitors a system or application log files. These systems respond with an alarm or countermeasure when a user attempts to gain access to unauthorized data, files, or services.

The intrusion detection market has created an emerging classification of products referred to as intrusion prevention. These products are similar to traditional NIDS and HIDS, but are designed to instantaneously act on attack detection by automatically blocking malicious activity before damage occurs.

IDS technology uses two basic complementary classifications of intrusion detection:

- Knowledge-based systems: This class of IDS products applies the knowledge accumulated about specific attacks and system vulnerabilities.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- Behaviour-based systems: These products assume that intrusions can be detected by observing a deviation from normal or expected behaviour of the system or the users.

### 8.4.2 Security vulnerabilities addressed by this technology

An IDS serves as an active monitor similar to the way guards and video can monitor a site's physical premises. It protects a computer or network of computers from misuse both inside and outside the network.

This technology provides security protection for the IACS environment by executing the following actions:

- monitoring access to and from a network;
- recording information useful for traffic monitoring and threat analysis;
- detecting, alarming, responding, or preventing attacks on the network or computers on the network.

### 8.4.3 Typical deployment

There are three ways in which all classifications of IDS can be deployed:

- NIDS: Passive sniffing through a promiscuous interface on network subnets. This interface watches all traffic on the particular subnet(s) to which the IDS is attached and compares traffic against a set of rules that determine whether the traffic indicates an attack. This technique is the predominant method of deploying NIDS.
- NIDS: Inline deployment where the NIDS functionality is in the forwarding path of the computer communications. This process is handled by embedding NIDS code in routers, firewalls, and stand-alone NIDS appliances.
- HIDS: IDSs are installed on each machine to monitor and audit actions on the computer and compare them to the HIDS policy.

A NIDS acts as a defence device by monitoring network traffic for threats exploiting known vulnerabilities on computers on the network. NIDS can perform important logging and auditing functions by providing alarms for attacks against these vulnerabilities and capturing the attack traffic that triggered the alarm. NIDS can have a variety of response actions in promiscuous mode, including implementing blocking policies on firewalls, routers, and switches, as well as resetting transmission control protocol (TCP) sessions that are carrying an attack. When deployed inline, NIDS also gain the ability to drop traffic that matches an attack signature and prevent the attack from exploiting the vulnerability. This new ability is reflected in the term “intrusion prevention systems” being introduced into the market.

HIDS involves loading software on a computer and having that software perform a variety of functions in order to detect and prevent attacks on the computer. HIDS systems vary in their technique for detecting intrusions. Typical applications include:

- monitoring traffic in and out of the computer;
- performing file integrity checks;
- monitoring suspicious user or application behaviour.

Some HIDS, referred to as “intrusion prevention” systems, can also prevent an attack using these techniques.

Best practices recommend that an effective intrusion detection system involves deploying both host and network IDS.

### 8.4.4 Known issues and weaknesses

An IDS can only protect the network and workstations on which it is installed. In many instances, an IDS is not installed on every subnet or computer within a network. The total cost

IECNORM.COM : Click to view the full PDF of IEC TR 62443-3-1 ed 1.0:2009

usually becomes the limiting factor in deploying IDS on a large scale. Total cost includes the cost of the IDS itself, certification and deployment costs, and operational costs to effectively monitor and maintain the IDS.

If the IDS is properly configured, it is an effective means for detecting, reacting to, or preventing attacks. However, an IDS can also be the single point of attack. With skill, hackers may be able to:

- identify an IDS through port scans or attacks prevented by the IDS;
- create a denial of service attack against the IDS;
- evade the IDS through a variety of techniques including encryption, fragmentation, or string obfuscation/manipulation.

Other issues with using IDS include:

- The cost of filtering false positives - False positives occur when an IDS sends an alarm that reports a benign activity as malicious and requires a response.
- Friendly fire - When enabling response actions of an IDS, a high level of accuracy is required to ensure that only malicious activity is blocked and that legitimate traffic gets through.
- High bandwidth networks might overrun the sensing capability of a NIDS.
- Lack of standardized testing procedures leads to large differences in the performance of IDS depending on traffic profiles used in testing.

The IDS technology is starting to inherit the title of security panacea, which can potentially provide a false sense of security. An IDS shall be looked at as being only one part of a larger network security approach. Deploying an IDS does not remove the need to implement other network security best practices, such as implementing access policy (firewalls), software controls on internal networks (antivirus), or proper host security on servers (patches, authentication, and authorization). Operators shall have the capability to easily configure and monitor an IDS for it to be effective. Developing effective IDS deployment, monitoring, and response actions requires an IT professional specifically trained on network security issues as well as the control system network.

### 8.4.5 Assessment of use in the industrial automation and control systems environment

In the IACS environment, NIDS are most often deployed between the PCN and the corporate LAN in conjunction with a firewall. HIDS are most often deployed on the computers that use general-purpose operating systems or applications. Properly configured, an IDS can greatly enhance the security management team's ability to detect attacks entering or leaving the system, thereby improving security. They can also potentially improve a PCN's efficiency by detecting non-essential traffic that goes to or from the network.

Other possible deployments include using either HIDS or NIDS in front of or running on individual control devices.

Issues faced when deploying IDS in Industrial Automation and Control System environments include the following:

- The lack of IDS products available for non-IP based protocols such as Foundation Fieldbus®, PROFIBUS®, or any serial-based network.
- The lack of HIDS products available for typical controller-based operating systems found on PLCs, RTUs, and DCSs.
- Incompatibility of HIDS products with Windows® or UNIX® control system software.
- The lack of IDS product support for IACS application layer protocols such as CIP™ or Modbus/TCP®.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- The lack of experience in the design of IDS policy and operation of the IDS suitable for industrial applications.
- Potentially significant overhead required to manage IDS in widely dispersed systems typical of SCADA environments.

### 8.4.6 Future directions

Future directions include the following:

- distributed IDS;
- false positive reduction;
- Future research and development needs to focus on Host Intrusion Detection/Prevention (HIDS) technology for detecting unauthorized activity without consuming the server's resources, interfering with control function, or adding latency. Agents that run on dedicated devices without introducing significant latency are examples of HIDS configurations that should be explored. Most control network traffic is static in the sense that the communication traffic is much more predictable and constrained then on a standard IT enterprise system; therefore, R&D needs to focus on testing devices that have anomaly detection capabilities (i.e., unauthorized access attempts and failed logons are examples of events that can be detected using HIDS). Extensive testing needs to be performed.

### 8.4.7 Recommendations and guidance

IDSs used to protect control systems should initially be configured so they do not have response actions for either incoming or outgoing traffic. The default configuration should only be modified when the security management team believes that the IDS has a high degree of accuracy in its detection techniques.

### 8.4.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [SANS3]
- [NIST05]
- [Pet2]
- [Mix]
- [Woold]
- [anon01], [anon02], [anon05], [anon35]
- [AW]
- [HLCCS]
- [SLL]
- [CY]
- [Rak]
- [KCS]
- [DNvHC]
- [Loc]

## 8.5 Vulnerability scanners

### 8.5.1 Overview

Vulnerability scanners provide network and systems administrators with a way to detect possible vulnerabilities on systems and networks before they can be used by malicious intruders to enter a computer system, as well as a control system once the enterprise system

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

has been compromised. Vulnerability scanners identify three types of security issues: inadequate policies, misconfigurations, and software flaws. Once the weaknesses have been identified, the software supplies administrators with detailed information about the vulnerabilities and the best means of securing them.

The two primary purposes for employing a vulnerability scanner are:

- Increasing security across an enterprise: Vulnerability scanners are used on enterprise networks to ensure a standard level of security exists across the enterprise network. The scanners identify weaknesses across the enterprise, generate security reports for each system or security statistics for the enterprise, and deploy patches or security configuration changes to vulnerable systems. Enterprise scanning of this sort is used to decrease enterprise risk levels and set a general level of basic security for each host without sacrificing a great deal of functionality.
- Verifying the security on specific high-risk systems: Targeted scans are performed against specific high-risk hosts or appliances. Vulnerabilities detected on the hosts are individually assessed for criticality and weighed against the functionality requirements of each system. To achieve a maximum balance between functionality and tight security, targeted scanning requires a high level of skill and knowledge from both the security administrator, who performs the scans, and the systems administrator, who maintains the system. Targeted scanning is designed to harden a high-risk system, decreasing the risk level to individual systems as much as possible.

The second purpose is of greater concern in a control system environment.

Vulnerability scanners usually consist of four primary components:

- Vulnerability database: Contains vulnerability information that typically reference Computer Emergency Response Team (CERT®) or vendor advisories and uses standard common vulnerabilities and exposure identification.
- Scanning engine: Performs three tasks: 1) detects devices on the network, 2) identifies the operating systems and applications resident on each computer, and 3) tests each system for vulnerabilities based on the identified operating system, applications, and security configurations.

NOTE 1 The configuration of the system being scanned and the design of the vulnerability scanner determine how vulnerabilities and misconfigurations are detected.

- Agent with local administrative privileges: Deployed on each host, similar to an antivirus client. Agents allow scan administrators to control when scans are run, determine what vulnerabilities to check for, and send results back to a centralized report repository. Agents are generally deployed when scans shall be performed regularly and enterprise security is a priority as opposed to specific host level security.

NOTE 2 While most vulnerability scanners have agents that can be deployed to the host, scans can still be performed without them although certain ports, services, and rights are required to do so in lieu of the local administrative access of the agent.

- Reporting mechanism: Lists the vulnerabilities found on each system, supplies details about each problem, and provides recommendations for resolving the identified security issues. Information about user accounts, open ports, and services running on each host are also included in the reports.

### 8.5.2 Security vulnerabilities addressed by this technology

Scanners check for the following three types of security issues on computer systems:

- Security policy weaknesses: Can be changed on individual systems, but do not relate to service or application configuration and software flaws. Such problems can be resolved by changing the policies on each host. Examples of these weaknesses include a lack of logging or auditing by the host, bad password policies, and poor control of user access and rights.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- Misconfigurations: Vulnerabilities that are based on the improper configuration of services, applications, or operating system components. Misconfigurations can be rectified by correcting how the software is implemented on each host. Examples of misconfiguration vulnerabilities include installing unneeded components or leaving unnecessary services running on the system.
- Software flaws: Actual design glitches in the operating systems, applications, or firmware. The only ways to resolve these vulnerabilities is to install patches or updates released by the vendor or use an external protection, such as a packet scrubber, to block access to the hole. Common examples include memory attacks such as buffer overflows on the operating system or injection attacks against databases.

### 8.5.3 Typical deployment

IT security personnel typically scan networks and devices as part of routine vulnerability testing and security assessments. These scans are used to determine the security posture and policy violations, such as failure to apply security patches or unsecured configurations.

The level and type of security needed (general standard security across the enterprise versus highly customized protection for high-risk hosts) determine which type of scanner is implemented on the network and how the scans are administered.

Enterprise scanners making use of host-based agents deployed are best for networks requiring standard levels of security, centralized security management and reporting, and patch deployment capabilities. Vulnerability scanners that run without an agent to assess or verify a system's level of security are best for evaluating high-risk systems such as control system components.

### 8.5.4 Known issues and weaknesses

The greatest limitation with the current generation of vulnerability scanners is the need for highly skilled security administrators and systems administrators. Scanning the hosts properly, interpreting the scan results, then implementing the fixes without disrupting services or opening new vulnerabilities requires the following qualities:

- strong familiarity with the operating system and its networking components;
- good understanding of the application and its environmental prerequisites;
- awareness of how the patch should interact with the application and operating system and what the possible consequences of the upgrade may be.

Another concern is accidental denial of service to devices and networks. Vulnerability scanners often attempt to verify vulnerabilities by extensively probing and conducting a representative set of attacks on devices and networks. Because current scanners have not been customized for control system environments, the manner in which scans are implemented could cause systems to shut down or fail.

False positives or negatives could be generated in the report. The scanner could incorrectly report that a vulnerability exists when it does not, a false positive; or that a system is not vulnerable when it really is, a false negative.

### 8.5.5 Assessment of use in the industrial automation and control systems environment

Ideally, targeted scans without use of the agents should first be run against development or test control system networks, isolated from production machines, in order to evaluate the impacts of the scans. Using the scanners against production networks should be performed carefully after they have been tested on backup systems. This recommendation, though, is simply best business practice for scanning any type of critical system, regardless of whether it is an IT computer or control system computer.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

Using vulnerability scanners to deploy patches or update software is not recommended for two reasons. First, neither users nor vendors of control systems have adequately implemented policies and techniques for patch management and software deployment. Until this issue is addressed, central deployment of patches should not be performed by vulnerability scanning software. Second, vulnerability scanners should verify the security of the host, not manage patch deployment, on high-risk systems. The deployment and vulnerability assessment processes should remain separate for computers that require a high level of security.

### 8.5.6 Future directions

Scanner databases and published vulnerabilities on industrial devices are currently limited with regard to IACS-specific vulnerabilities. This lack of information further limits the effectiveness of scanners to identify vulnerabilities in IT operating systems and applications. However, given the industry move towards standard IT operating systems and applications, and away from air-gapped systems, scanners can help enhance the level of security on those IT components. Tests for control system-specific vulnerabilities can eventually be included in the scanners.

### 8.5.7 Recommendations and guidance

Vulnerability scanners should be used in control system environments that have deployed standard IT operating systems or applications. Their use should be carefully monitored on a backup network in order to minimize the chance of taking a production network offline. Additionally, special attention should be paid to the vulnerabilities discovered in order to ascertain if false positives or negatives have been generated. Finally, any changes or updates made to secure the hosts should be done on backup or test systems to identify any possible harmful repercussions before the fixes are made on production control systems.

The use of vulnerability scanners in control system networks could significantly improve host-based security in these environments and provide a way of assessing risk levels on the network and on each individual host.

### 8.5.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Her]
- [anon09], [anon31], [anon34], [anon36],
- [FS]
- [And]

## 8.6 Forensics and analysis tools (FAT)

### 8.6.1 Overview

FATs passively gather data about a network and its structure, traffic, and users by analyzing raw network packets. These tools are used to baseline network activity, analyze unusual network traffic, and help security researchers and control system (CS) network administrators. The three types of network analysis tools addressed in 8.6 are: (1) packet capture, (2) network monitoring, and (3) network forensics and analysis (NFA) applications. All network analysis tools work basically the same way. The difference lies in the reporting and management capabilities built into network monitoring and NFA software.

- Packet capture tools: Packet capture tools such as Ethereal®, EtherPeek®, or NetMon capture raw network packets as they go across the wire and display the packet information in granular detail for an analyst to review. They break out packet fields and header information into easily readable formats and can be used to show real-time activity on the network. Custom filters can be set to allow network administrators to capture packets based on protocol type, IP address, etc., allowing the administrators to weed out information irrelevant to their task. Packet capture tools can be used to troubleshoot networking issues, examine anomalous behaviour closely during incident response, or help

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

administrators or researchers understand why individual system events generate the network traffic they do.

- Network monitoring tools: Commercial network monitoring and analysis tools, such as Hewlett Packard OpenView, extend the capabilities of a packet capture tool for use on an enterprise network. Network monitoring applications work in a similar fashion to packet capture software. However, they monitor the health of enterprise networks, have extended analysis and reporting capacity, and may allow network administrators to centralize network management functions.
- Forensics and analysis tools (FATs): FATs function similarly to network monitoring tools because they provide enterprise monitoring of an enterprise network, centralized network security management functions, and extensive reporting capacity. They differ from network monitoring and packet capture tools because they are designed as a defensive measure rather than a network administration tool. While NFA applications monitor traffic, they also baseline normal traffic from a network security perspective and can be configured to perform certain actions in response to detected security events.

### 8.6.2 Security vulnerabilities addressed by this technology

Network analysis applications are critical for detecting unusual network communications, performing CS network administration, and responding to computer security incidents. While packet capture and network monitoring tools may not provide active defensive measures on a network, they do provide critical information needed during network disruptions and for computer incident response.

This type of software addresses a general need in control system security rather than a specific vulnerability. The relative lack of documentation of older or proprietary CS network protocols requires the use of network analysis tools by security researchers. In order to analyze how the network protocols and CS applications work, security researchers and CS application vendors shall have the tools necessary for network protocol analysis.

### 8.6.3 Typical deployment

In a control system environment, network analysis software can be used to establish a baseline of normal network communications, a task that helps facilitate incident response and risk assessment. The establishment of traffic baselines through packet analysis on the CS network is necessary for detecting anomalous traffic, and for performing successful incident response. If the normal traffic patterns have not been assessed, then verifying what is anomalous becomes much more difficult and hinders incident response capabilities.

Once irregular network traffic has been captured and analyzed by network analysis software, security personnel and network administrators use the data dumps to evaluate what is actually happening on the network. Anomalous traffic is compared to baseline traffic to provide critical information about which hosts are generating the traffic, which ports and services may be involved, and which network protocols are being used. Packet dumps of uncharacteristic traffic can be used to ascertain whether the traffic is due to network issues, system misconfigurations, or a compromised system.

### 8.6.4 Known issues and weaknesses

For industrial automation and control environments, with their unusual protocols (e.g., fieldbus, OPC), network configurations (e.g., SCADA) and data constructs (e.g., OPC-DA, Alarm and Event, Batch and DCS messages), there are few commercial tools available for purchase that can satisfactorily cover the forensics task. The system administrator is left with creating localized tools for specific protocols to cover the gaps between standard business network FATs capabilities and control system needs. Fortunately, data historians can provide some ready-to-use capability for high-speed capture and storage including some analysis tools to assist the system administrator.

Commercial tools tend to be limited to the choices based on a threat environment current at the time the tool is designed. Additionally, commercial tools are immature at this point relative

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

to the virus protection tools, which have sophisticated commercial licensing and database update models.

FATs require the systems administrator to configure the tool to look for and collect the data for a given set of threats. If the FAT is not looking for the data that corresponds to an attack, or only captures part of the attack in process, then the investigator is left with an incomplete picture of the attack. Not only does configuration play a part in the data collection issue, but also the difference between the rate at which networks process data relative to the rate that they can persist data to a storage medium. FATs cannot hope to then store every piece of data and shall work with a subset of the complete pathology of each attack. This data reduction then comes either using some form heuristics or compression at the source of the message or would demand significant amounts of shared memory to buffer data before releasing to persistence upon an attack. This latter approach is the same way that an aircraft 'black box' captures data continuously until a serious event occurs, then writes to hardened storage for some time after the event. In each case, the system administrator needs to apply logic to define which data reduction rules shall be in effect and which attacks or pattern of attacks to watch for.

Finally, FATs are themselves subject to the same privacy laws in control environments that business systems find themselves working under. In the current climate, these laws vary considerably from country to country.

### 8.6.5 Assessment of use in the industrial automation and control systems environment

FATs do not yet support industrial protocols. As a result, their use in an IACS environment is now limited to workstations connected to an Ethernet network using traditional IT protocols. They should be used with care on an operational IACS network.

### 8.6.6 Future directions

There is a need for FATs to be adapted to common IACS protocols, such as OPC and fieldbus protocols. Filtering and data reduction tools shall also be adapted to the kinds of data flows more common to the manufacturing environment.

The kinds of advanced data analysis techniques that industry has built for complex problems, such as inferential sensing, control system model identification, etc., could be applied to the FATs used in IACS environments. For example, an attack on a control system could take the form of one or more field instruments being spoofed to induce a shutdown of a piece of equipment. Forensic tools that use statistics, neural nets or other inferential techniques could then be used to discern that the data combinations were not possible instrument readings and identify the source of the attack.

Other advanced tools, such as online analytical processing data cubes, need to be applied to FAT data to manage the large increase in data that will need to be analyzed as networks become more complex. An active IDS can be used to provide an input to the FATs by providing triggers and real-time configuration changes to a FAT to adapt the forensic data collection as an attack gets underway.

Finally, the direction of privacy and counterterrorism laws will dictate some of the boundaries and the obligations of system administrators for the foreseeable future.

### 8.6.7 Recommendations and guidance

FATs should always be deployed in tandem with an active IDS. The logic used to configure an IDS can be applied to a FAT. The threat environment that the IDS faces will always provide a subset of the data required for an effective FAT deployment. The system administrator should therefore prepare for a FAT deployment with a comprehensive threat assessment.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

In using a FAT, the hardest decisions will be to manage the trade-offs between the amount of data and where it is collected from, the persistence space required to collect enough information to reconstruct the attack or incident, and the data reduction techniques used to manage the rate and quality of the data being persisted.

When collecting and storing vital forensic data about either IACSs or users of those systems, be aware of and review the privacy laws and other laws in effect for the data to be collected. It can be considered illegal to collect too much data or to collect too little data depending on the industry, the use of the system and the laws in effect at the time.

#### 8.6.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [KW]
- [Gar]

### 8.7 Host configuration management tools (HCM)

#### 8.7.1 Overview

HCM tools are in use by systems administrators to manage resources centrally, control access to systems, and set a general level of security for each host on a network. These tools make it easier for administrators to track what software and hardware are available on each host and to set a standard software and hardware configuration, which often results in cost and time savings when managing the computers. To fully benefit from host configuration management tools, a network shall enforce strong policies for system use and security, have a fairly homogenous hardware and software environment, and be a large or very widespread network.

Industrial automation and control systems do not typically use HCM tools because of the policy-driven nature of the tools. Most of the configuration is done through the IACS application and is established because of functional needs rather than administrative or security policies. HCM on these networks is typically limited to one of two options: a) controlling user permissions and access, or b) limiting operational capacity strictly for performance-based needs. Any standardization of the hardware or underlying operating system is driven by the functionality requirements of the IACS application, not security concerns.

HCM tools and applications are commonly used in the general IT world because of the critical nature administration and security policies play in IT network management. The cost of not having policies in place and a means of monitoring or enforcing them is a great deal higher because of the large number of machines requiring administration and the greater number of threats to the networks.

#### 8.7.2 Security vulnerabilities addressed by this technology

HCM tools address no specific vulnerabilities related to IACSs and networks. Utilization of HCM software is a preventive measure because it provides a means of enabling and enforcing security and administration policies.

#### 8.7.3 Typical deployment

Industrial automation and control system operators do not use HCM tools. Instead, they use the IACS application to determine the host configuration. User access and restrictions can be set on each operator or engineering workstation via the IACS application, with each user granted a certain level of access to system resources based on his or her occupational requirements. Another method that operators use to manage host configuration is to load specific modules of IACS software, depending on the purpose of the machine. For example, ladder logic development tools are not needed on most operator workstations, so a separate module has to be loaded to allow data gathering, limited control of IACS units such as PLCs or RTUs, and alarm monitoring.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

IT HCM tools vary depending on the operating systems being managed. Predominantly Microsoft Windows® shops use Active Directory and other third party tools to manage resources, track assets, and manage policy enforcement. HCM is very centralized and administered to the network as a whole. LDAP, Network Information System, and Network File System are similar solutions used in the Linux® and UNIX® world, but they are not popularly deployed. Most HCM tasks for Linux® and UNIX® are managed through the use of customized scripts and remote administration tools.

### 8.7.4 Known issues and weaknesses

The biggest issue presented by the use of HCM tools in an IACS environment is the lack of standardized software and hardware on most of these networks. HCM tools are not cost effective or practical if the computing environment is not standardized and does not need to be. Policy could be set and enforced more easily on a system-by-system basis through the use of remote administration tools. The adoption of a UNIX®/Linux® approach to HCM would prove more effective.

Second, most HCM tools are designed to oversee the configuration of an operating system and its components, and to manage user access to system resources. Most IACS software does not support significant or frequent changes to an operating system or applications such as web servers and databases. Additionally, user access and restrictions are generally controlled through the application rather than the operating system.

### 8.7.5 Assessment of use in the industrial automation and control systems environment

Currently, the base configuration of the operating system and its components on an IACS system are not closely controlled for security or administrative purposes. The requirements of the control application drive the host's configuration because the applications are operating system and component dependent. Since HCM tools are employed to control the configuration of the operating system and related applications, they will not be cost effective or practical until the architecture of control applications changes significantly.

IACS operators and vendors should begin to evaluate current administrative tasks and upcoming changes in application software, though, for tasks or procedures that need to be standardized. As the nature of IACS software changes with the integration of commercial off-the-shelf (COTS) operating systems and applications, the need for strong administration, change control, and security policies will increase. IACS operators and vendors should begin evaluating their systems, tasks, and procedures for areas where policies may be enacted to strengthen network integrity.

### 8.7.6 Future directions

IACS networks are beginning to include more COTS software, become more standardized, incorporate more plug-and-play capabilities, and focus on security. As these changes occur, HCM of the base operating system and application components such as web servers and databases will need to be updated, subject to more version control, etc., administrative tasks not currently performed on IACS networks frequently. IACS vendors and developers should begin to evaluate the need for managing host configurations and determine their customers' specific HCM requirements.

### 8.7.7 Recommendations and guidance

IT HCM tools, specifically their functionality and architecture, are likely to be ported over for use on IACS networks as more COTS software and common standards are employed. To this end, IACS application vendors and developers should understand how HCM tools are used, what the requirements are for using them effectively, and if their use justifies the cost. But until IACS environments become more standardized and require strong administration and security policies, IACS operators should consider what administrative and security tasks could benefit from standard HCM and what policies would be needed to manage them.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 8.7.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography

- [anon11], [anon12], [anon15], [anon16], [anon21], [anon22], [anon25], [anon27]

## 8.8 Automated software management tools (ASM)

### 8.8.1 Overview

ASM tools are applications used to distribute software across a network to specified hosts or groups of hosts. The kind of software that can be deployed by the ASM tools depends on the type of ASM application being used. There are two categories of ASM applications and a third informal type, which is a client-side module included in most COTS software.

ASM tools are becoming popular on networks of all sizes because of the significance they play in centralizing and facilitating administrative and security tasks. Software lifecycle management, application version control, and patch management are now priorities on IT networks for a number of reasons, including:

- The incredible complexity of managing multiple versions of enterprise applications and software on a network.
- The increasing importance of software lifecycle management and the cost of supporting out-of-date products.
- The need for rapid testing and deployment of security patches and fixes to prevent widespread attacks on a network.

The first ASM application category is an enterprise application suite used to deploy major software packages across the network. It can be used to manage versions of operating system components, update third party applications, push security fixes and patches, and control general lifecycle software requirements for the organization. These ASM applications can be very expensive and resource intensive (time, administrative, and physical), so they are typically used on large networks or by organizations that frequently deploy software across an enterprise and require centralized control of their systems and their configuration. Examples of this kind of ASM software include Microsoft SMS, Altiris, ManageSoft, and LANDesk products.

The second category is a third party application used to update a very limited range of products. Patch management software is the primary example of this sort of ASM application. It is used to evaluate systems for vulnerabilities and deploy patches or updates to fix the problems. Due to the short cycle of vulnerability detection and patch installation on most IT networks, centralized control and distribution of security fixes is critical. Many small networks or organizations that need to deploy patches to a targeted group of systems within a large network use patch management applications. Examples of these kinds of ASM tools include Patchlink, Microsoft WUS, and Shavlik HFNetChkPro.

The third informal type of ASM tool is the update components that most major COTS software vendors include with their products. These are client-side modules bundled with the application to make sure the application is up-to-date for both security and functional purposes. These modules are available or included in applications such as antivirus products, operating systems, and other COTS products. Examples of applications using client-side modules for updating software automatically are RealPlayer, Adobe Acrobat, all antivirus products, Windows® Update services, Red Hat Linux® RHN, and Debian Linux® apt-get.

### 8.8.2 Security vulnerabilities addressed by this technology

ASM tools facilitate the deployment of security updates and patches for operating systems and applications, fixing holes through which attackers can penetrate a network. Keeping software updated for version control and lifecycle management purposes is important for security and functional reasons.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 8.8.3 Typical deployment

ASM tools are currently deployed in a limited fashion on IACS networks. ASM software may or may not be used by IACS application vendors to handle updates, but some client-side applications are being employed to manage updates to antivirus and firewall software, which are loaded on hosts running new applications. The implementation of the client-side agents is closely controlled via policy and implementation to prevent interference with the application, and to restrict how updates are downloaded and deployed on the IACS networks.

As COTS operating systems and applications become integrated into more IACS environments, ASM tools will be thoroughly evaluated for patch management and application version control purposes. ASM suites designed to deploy enterprise applications are not being implemented because they are not suited for administrative or security tasks on most IACS networks at this time.

### 8.8.4 Known issues and weaknesses

ASM deployment and update processes shall be carefully examined to ensure the update process itself does not interfere with the IACS functionality. Because these applications require administrative access to a host and dedicated physical resources on a host, loading agents for any of the three ASM categories should be monitored and tested thoroughly before deploying them on production systems. The agent software itself could disrupt system functionality.

A well-defined testing and deployment procedure should be developed to determine which updates should be applied and how they should be tested before they are placed on a production system. Testing is critical on IT networks, but it will play an even greater role when deploying software on IACS hosts.

Since ASM tools often pull updates from external websites, the architecture and communications of the applications should be carefully considered before employing them on protected networks. The tools could introduce new paths or vulnerabilities onto IACS networks that will need to be secured or removed.

The integrity of the data being pulled down for updates should also be reviewed before being applied to IACSs. Introduction of corrupted or malicious data could impede IACS capabilities or compromise a system.

### 8.8.5 Assessment of use in the industrial automation and control systems environment

Client-side agents or modules that manage application updates are already being employed in IACS environments because they do not interfere with the performance of the IACS. These tools are being put into operation for application updates related to the antivirus software and firewalls, but they can also be used to manage application version control of web-based console components or for the IACS application updates.

As patch management becomes an important consideration with IACS vendors, third-party applications designed to deploy security updates may be evaluated and tested for use. The patch-specific ASM tools are well suited for IACS networks because these networks are often widespread and are already centrally administered. This type of technology lends itself well on networks with fewer hosts requiring patches, as is the case in most IACS environments, and is very cost-effective.

Enterprise ASM suites will probably not be applied on IACS networks because they are designed for large networks whose systems all have enterprise applications and require patching.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

### 8.8.6 Future directions

Client-side update agents or modules will become more prevalent as COTS software is deployed on IACS networks. As patching becomes more important, security-specific ASM applications will become more common. Widespread employment of security-specific ASM tools will, however, not occur until applications are able to handle the frequent patch cycles typical on an IT network.

### 8.8.7 Recommendations and guidance

IACSs operators and vendors need to review closely the potential utility of these tools as COTS software is more heavily employed on their networks. Testing and software management policies should be developed to support the tasks and clearly define what software updates are really needed. Once the ASM tools have been deployed, the hosts and network should be re-evaluated in case the tools introduce new security concerns.

### 8.8.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography

- [anon13], [anon14], [anon17], [anon18], [anon19]
- [anon20], [anon23], [anon24], [anon26], [anon28]

NOTE Many of these references are product specific, but the case studies and general information about the tools provide good predictive guidance for the use of ASM applications on IACS networks.

## 9 Industrial automation and control systems computer software

### 9.1 General

The software used in IACS equipment is a vital factor in determining the overall security of a control system. It provides a certain degree of protection by mediating access to devices, but can also be a source of vulnerability due to programming errors (such as buffer overflows) or inattention to security issues during the development process.

Clause 9 examines security of three key software components used in IACSs:

- Server and Workstation Operating Systems;
- Real-time and Embedded Operating Systems;
- Web Servers and Internet Technologies.

This clause does not discuss security of individual IACS application programs.

The operating system (OS) is the most important program that runs on a computer. Every general-purpose computer has an OS that performs basic tasks, recognizes input from the keyboard, sends output to the screen, keeps track of files and directories on the hard disk, and runs other software applications loaded on the computer. On large computers, the OS also has the responsibility to make sure that different programs and users do not interfere with each other. The OS is also responsible for ensuring that unauthorized users are not granted access to the system.

Web and Internet technologies are becoming increasingly popular in IACSs because they make it easy to distribute timely production information to users outside the control room. However, they also make IACSs more susceptible to cyber attacks due to the high number of vulnerabilities in the technology at its current stage of development.

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

## 9.2 Server and workstation operating systems

### 9.2.1 Overview

An OS is the foundation software of a computer. It typically schedules tasks, allocates storage, and provides the following services:

- a default user interface when no applications are running;
- an application programming interface for software development;
- an interface to the machine's hardware and peripherals.

### 9.2.2 Security vulnerabilities addressed by this technology

The OS is the last line of defence to protect applications and sensitive information. It typically identifies and authenticates each user through a login and password mechanism and determines what resources (files, applications, and communications ports) are accessible to the user. It can provide auditing services to record security events and actions (logon, logoff, resource access, and configuration changes). An OS typically provides a mechanism that ensures that only designated persons can make changes to system configurations and security policies.

### 9.2.3 Typical deployment

In the IACS environment, SCADA hosts, plant computers, and HMI stations typically use the same server and workstation operating systems common to the IT world (mainly Windows® and UNIX®). PLCs, RTUs, DCS controllers, and other data acquisition equipment typically use specialized real-time or embedded operating systems.

The remainder of 9.2 deals with server and workstation operating systems, while 9.3 covers real-time operating systems.

### 9.2.4 Known issues and weaknesses

The UNIX®, Linux®, and Windows® operating systems base security on the concept of discretionary access control (DAC) and provide two categories of user:

- an administrator who has full access to all system resources;
- ordinary users who have full access to the applications and files they need for their jobs.

DAC does not enforce a system-wide security policy, and protective measures are largely under the control of individual users. Any program run by a user inherits all the permissions of that user and is free to modify any files the user can access. Therefore, DAC-based operating systems are susceptible to virus and Trojan attacks.

Additional OS weaknesses are caused by:

- poorly chosen passwords—passwords that are easy to remember (because they are short, or use a dictionary word) are also easy to crack;
- default or infrequently changed passwords;
- unseen security risks caused by modern operating systems that install services that automatically connect to the network;
- remote access to servers on a network.

### 9.2.5 Assessment of use in the industrial automation and control systems environment

Server and workstation OSs are widely used in the IACS environment at the operator HMI, plant computer, and supervisory control levels. These OSs are also used extensively in IT

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009

applications, although IT security policies may require modification to suit the needs of control systems.

Security policies shall balance the need for protection against the need for users to easily access required applications. In an office setting, a temporary inability to access email or run a spreadsheet is not a serious issue. In the IACS environment, in contrast, it is often critical that operators have immediate access to systems and applications. Therefore, security policies that lockout users after a certain number of failed password attempts or rapidly age passwords requiring them to be changed frequently are likely to be inappropriate. IACS operating system security policies should also take into account physical security (see Clause 10), as access to control centres is frequently limited to authorized personnel only.

Policies regarding applying patches to OSs components create another situation where standard IT procedures do not fit the IACS environment. The patch may remove vulnerability, but it can also introduce a greater risk from a production or safety perspective.

### 9.2.6 Future directions

High-security versions of popular OSs, such as Microsoft Next-Generation Secure Computing Base, National Security Administration (NSA), Security Enhanced Linux®, and Hewlett Packard Secure OS for Linux®, are beginning to appear. These systems currently incorporate one or more of the following security concepts: encrypted file systems, disabling of unnecessary network ports, and client-side firewalls. More sophisticated security technologies include:

- Strong process isolation: Protecting pages of main memory so that each application can be assured that it is not modified or observed by any other application, even the operating system.
- Sealed storage: Ensuring that only the application that saved data (or a trusted designated application or entity) can open it.
- Secure channels: Allowing data to move safely from the keyboard/mouse to applications, and from applications to a region of the screen.
- Attestation: Enabling users to authenticate software or a combination of software and hardware, based upon a cryptographically identified trusted software stack.
- Mandatory access control: Providing the means for a central administrator to apply very fine-grained access policies that are enforced by the operating system.
- Isolated security domains: Preventing unauthorized communication between programs to limit damage from an attack.
- System event auditing: Providing a full security audit trail.
- File system integrity: Checking for signs of tampering.

### 9.2.7 Recommendations and guidance

Recommendations and guidance for OS security are highly dependant on both the system and environment. However, two general recommendations are the following:

- disable all unnecessary services;
- change the vendor's default passwords.

### 9.2.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [NIST08], [NIST13]
- [anon33]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

## 9.3 Real-time and embedded operating systems

### 9.3.1 Overview

Operating systems form the foundation software of a computer and those workstations used in a control environment. They typically schedule tasks, allocate storage, and provide an application programming interface for software development and an interface to the machine's hardware and peripherals.

A real-time operating system (RTOS) guarantees that interrupts are handled within a certain specified maximum time, thereby making it suitable for control and other time-critical applications. Typically, an RTOS is deployed in embedded systems that have severe resource constraints compared to conventional desktop or workstation computers. In addition to time-based constraints, they are designed for hardware environments where:

- there is limited memory capacity;
- programs are loaded from a read-only memory or flash memory device;
- no disk is available for data and program storage;
- processor power is limited (8 and 16 bit processors are still common in many embedded applications).

### 9.3.2 Security vulnerabilities addressed by this technology

In an embedded application, the RTOS is the last line of defence to protect applications and control outputs from external attacks or someone gaining unauthorized access to a remote site where the embedded device is located. If the device has a user interface, it is likely to be protected by a simple password mechanism.

### 9.3.3 Typical deployment

RTOSs are widely used in IACSs as key software in data acquisition and control equipment such as RTUs, PLCs, IEDs, and DCS controllers.

These systems typically have a variety of digital, analog, and pulse counter input and output ports connected to sensors and actuators that monitor and control a physical process. They also have at least one network connection that serves as the main interface to the device from host computers running HMI, SCADA, or control software. Network connections may be serial interfaces for devices located at remote locations using radio or telephone links back to a central site. Other devices support specialized industrial networks, such as Foundation Fieldbus®, PROFIBUS®, and ControlNet®. Increasingly, embedded systems provide a TCP/IP network connection and incorporate Internet services such as email, FTP file transfers, and even Web servers.

These network connections are used to:

- request data transfers from the device (polling);
- transmit data or event notifications to the host computer (report by exception);
- download operating parameters such as alarm limits and setpoints;
- switch outputs on or off or, in the case of analog output, adjust its value;
- download new or updated application programs.

### 9.3.4 Known issues and weaknesses

Generally, RTOS designers have not placed security as a high priority compared to the other constraints with which they have to deal. Most embedded controllers use software, operating systems, and communication protocols that are not commonly available or accessible. While obscurity may have been an adequate defence in the past, two things have changed:

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed 1.0:2009

- The majority of new embedded systems are Internet enabled and some even feature wireless access for convenience.
- The nature of the threat has become more serious. There is increasing concern that cyber terrorists will target embedded applications because they are often connected directly to physical processes.

Most RTOSs have no mechanism for denying access to system resources unless there is a timing conflict. Embedded systems typically use a flat memory space that is available to all processes. As a result, malicious programs that are introduced into an embedded device (e.g., through its network connection) are free to read and modify any data and cause havoc with the normal operation of the device.

Other issues include:

- using default or infrequently changed passwords on devices with user interfaces;
- inadequate resources in the RTOS kernel for using security applications;
- appropriate interrupt priorities that include security.

#### 9.3.5 Assessment of use in the industrial automation and control systems environment

For the IACS environment, “edge” devices like RTUs, PLCs, and controllers are arguably as important as, or more important, than the host computers. They perform measurement functions, make logic and control calculations, and issue commands that modify the operation of the process. These devices are embedded computers that rely on a RTOS for their basic operation. Furthermore, the nature of industrial control requires that these devices accept parameters, commands, and even downloads of new programs through a network connection.

The combination of limited internal security features, plus the requirement that devices accept commands sent over the network, make these systems vulnerable to cyber attacks unless they are on a truly isolated network. The problem is further aggravated by the trend to Internet enable these devices for Internet connectivity by adding convenience features like web servers for remote administration.

#### 9.3.6 Future directions

Derivatives of Linux® and Windows® desktop operating systems, with real-time characteristics, are beginning to appear in embedded applications. While these operating systems may be more familiar to potential attackers then a specialized RTOS, they also provide more security features.

As network-connected embedded devices become universal, security features will need to be developed and added to, or built into, the RTOS.

#### 9.3.7 Recommendations and guidance

It is important to carefully isolate communication networks used in IACS applications, especially if TCP/IP is used as the transport mechanism. One recommendation is to separate time-critical application traffic from information traffic (i.e., loading, diagnostics, and resource management) in order to limit vulnerability and possibility of attack. This method of isolation would limit access to information traffic by external users.

#### 9.3.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Mon]
- [Cor]

IECNORM.COM : Click to view the full PDF of IEC/TR 62443-3-1 ed1.0:2009