



D3.13 – i4Q Cybersecurity Guidelines v2

WP3 – BUILD: Manufacturing
Data Quality



i4Q has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 958205.

Document Information

GRANT AGREEMENT NUMBER	958205	ACRONYM		i4Q
FULL TITLE	Industrial Data Services for Quality Control in Smart Manufacturing			
START DATE	01-01-2021	DURATION		36 months
PROJECT URL	https://www.i4q-project.eu/			
DELIVERABLE	D3.13 – i4Q Cybersecurity Guidelines v2			
WORK PACKAGE	WP3 – BUILD: Manufacturing Data Quality			
DATE OF DELIVERY	CONTRACTUAL	31-Dec-2022	ACTUAL	30-Dec-2022
NATURE	Report	DISSEMINATION LEVEL		Public
LEAD BENEFICIARY	IKERLAN			
RESPONSIBLE AUTHOR	Aitor Uribarren and Maialen Eceiza (IKERLAN)			
CONTRIBUTIONS FROM	2-ENG, 4-ITI			
TARGET AUDIENCE	1) i4Q Project partners; 2) industrial community; 3) other H2020 funded projects; 4) scientific community			
DELIVERABLE CONTEXT/DEPENDENCIES	This document presents Security Guidelines (i4Q ^{SG}) sufficient cybersecurity procedures to assure data dependability and quality in a manufacturing line. This document is the updated v2 of D3.5 i4Q Cybersecurity Guidelines.			
EXTERNAL ANNEXES/SUPPORTING DOCUMENTS	None			
READING NOTES	None			
ABSTRACT	According to recent surveys, one of the top three corporate hazards is the fear of cyber-attacks. Cloud computing, privacy protection, mobility, and the internet of things are all driving forces in the realm of IT security in industrial settings. This document presents general description and technical application of i4Q Security Guidelines (i4Q ^{SG}) which intends to highlight important features of ICS cybersecurity, including best practices and key aspects for defending against an increasing array of cyber-related threats.			

Document History

VERSION	ISSUE DATE	STAGE	DESCRIPTION	CONTRIBUTOR
0.1	07-Nov-2022	ToC	ToC Draft and first input	IKERLAN
0.2	25-Nov-2022	1 st Draft	Available for Internal Review	IKERLAN
0.3	30-Nov-2022	Internal Review	Internal Review	TUB, BIESSE
0.4	02-Dec-2022	2 nd Draft	Addressing comments from internal reviewers	IKERLAN, TUB, BIESSE
0.5	09-Dec-2022	Final Draft	Submission for final draft for quality check	IKERLAN
0.6	19-Dec-2022	Update	Image update	IKERLAN
1.0	30-Dec-2022	Final Document	Final quality check and issue of final document	CERTH

Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

© i4Q Consortium, 2022

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

TABLE OF CONTENTS

Executive summary	8
Document structure	9
1 General Description	10
1.1 Overview	10
1.2 Introduction to IEC 62443 Standard.....	10
1.2.1 Scope and Purpose	11
1.2.2 Design principle: Secure by Design.....	12
1.2.3 Design principle: Reduce Attack Surface	12
1.2.4 Design principle: Defense in Depth	12
1.2.5 Design principle: Essential Functions	13
1.3 Introduction to ISO 27001 standard.....	13
1.3.1 Risk assessment methodology	13
1.3.2 Benefits of applying ISO 27001	14
1.4 Security strategies	14
1.4.1 Motivation	14
1.4.2 Strategies.....	15
1.4.3 Defense in Depth	15
1.5 Industrial security vs Functional safety.....	16
1.6 IT security vs Industrial security.....	16
1.7 Security Administration	17
1.8 Public/Private Certificates.....	17
2 Technical Specifications – Application	19
2.1 Installing a feeling of accountability.....	19
2.2 Layered protection	19
2.2.1 Risk analysis	20
2.2.2 Plant Security	20
2.2.2.1 Security check list.....	21
2.2.3 Network Security.....	21
2.2.3.1 Separation between production and office networks.....	21
2.2.3.2 Cell protection concept.....	22
2.2.3.3 Secured remote control for service and maintenance.....	22
2.2.3.4 Secured connection to cloud solutions	22



2.2.3.5	Security check list.....	22
2.2.3.6	Specific firewall for users.....	22
2.2.3.7	Security monitoring.....	23
2.2.4	System Integrity	23
2.2.4.1	Access protection for configuration.....	23
2.2.4.2	Access protection for runtime operations	23
2.2.4.3	Access protection for network components (Network)	23
2.2.4.4	System hardening	24
2.2.4.5	Updates and patch management.....	25
2.2.4.6	Whitelist.....	25
2.3	Public Key Infrastructure	25
2.3.1	Basic functions of the PKI	26
2.3.2	i4Q chain of trust	26
2.3.3	Certificate Management	27
2.4	Validation and Improvement.....	28
2.5	Updates/Patches in ICS.....	28
2.5.1	Considerations	28
2.5.2	Software Update strategies	29
2.5.3	Test and Validation	31
3	Implementation Status	33
3.1	Current implementation	33
3.2	History	33
4	Conclusions.....	34
	References	35
	Appendix I.....	36

LIST OF FIGURES

Figure 1. Security Management Process Cycle [8].....	17
Figure 2. i4Q PKI structure proposal.....	27
Figure 3. Layered network architecture	30

LIST OF TABLES

Table 1. i4Q ^{SG} Version history.....	33
--	----



ABBREVIATIONS/ACRONYMS

AES	Advanced Encryption Standard
AMT	Active Management Technology
AV	Antivirus
AWS	Amazon Web Services
BIOS	Basic Input/Output System
CA	Certification Authority
CIA	Confidentiality, Integrity, and Availability
CMMI	Capability Maturity Model Integration
CPS	Cyber Physical Systems
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSG	CyberSecurity Guidelines
CVE	Common Vulnerabilities and Exposures
DiD	Defense in Depth
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
DODIN APL	Department Of Defence Information Network Approved Product List
DSS	Decision Support System
EDR	Endpoint Detection and Response
EUC	Equipment Under Control
EWf	Expert Witness Disk Image Format
FTP	File Transfer Protocol
GCP	Google Cloud Platform
HMI	Human Machine Interface
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
i4Q^{SG}	I4Q Security handler
IACS	Industrial Automation and Control Systems



ICS	Industrial Control System
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
IoT	Internet of Things
LAN	Local Area Network
MAC	Media Access Control
MMC	Microsoft Management Console
MQTT	Message Queuing Telemetry Transport
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OT	Operational Technology
PC	Personal Computer
PDF	Portable Document Format
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
SaaS	Software as a Service
SCADA	Supervisory Control And Data Acquisition
SIAC	Safety, Integrity, Availability, and Confidentiality
SIF	Safety Instrumented Function
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security



UEFI	Unified Extensible Firmware Interface
UI	User Interface
USB	Universal Serial Bus
VA	Validation Authority
VLAN	Virtual Local Area Networks
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2
WSUS	Windows Server Update Services



Executive summary

This document presents an executive explanation of the **i4Q Security Guidelines v2 (i4Q^{SG})** Solution providing the general description and technical application. This document **i4Q Security Guidelines (i4Q^{SG}) v2** is an update of v1 of **Security Guidelines (i4Q^{SG})**, for this reason it contains information of the 1st version together with the updates developed in this 2nd version.

Many types of control systems are included in the term "industrial control system" (ICS). It includes supervisory control and data acquisition (SCADA), distributed control systems (DCS), and programmable logic controllers (PLCs), which are regularly used in industrial and critical infrastructure environments.

Security researchers pay more attention to ICS flaws due to increased attacks on infrastructure. Consequently, organizations could better identify and manage cyber threats presented in critical infrastructure with additional research into ICS vulnerabilities.

By presenting best practices and important aspects of defending against cyber-related threats, this guideline intends to emphasize important parts of ICS cybersecurity.



Document structure

Section 1: Contains a general description of the **i4Q Security Guidelines (i4Q^{SG})**, providing an overview and the list of main design principles. It is addressed to final users of the **i4Q Solution**.

Section 2: Contains the technical specifications of the **i4Q Security Guidelines (i4Q^{SG})**, providing an overview and detailed list of secure actions to apply. It is addressed to IT/OT administrators as well as software developers.

Section 3: Details the implementation history of the **i4Q Security Guidelines (i4Q^{SG})**, explaining the current status and next steps.

Section 4: Provides the conclusions.

APPENDIX I: Provides the PDF version of the **i4Q Security Guidelines (i4Q^{SG}) web** documentation, which can be accessed online at: http://i4q.upv.es/5_i4Q_CSG/index.html

1 General Description

According to recent research [1], one of the top three corporate hazards is the fear of cyber-attacks. Cloud computing, data privacy, mobility, and the internet of things are all key drivers of change in the field of IT security in industrial settings. The Industrial Internet of Things will not be adopted without IT Security.

Almost 22,000 vulnerabilities were published in 2021 [2]. The National Vulnerability Database (NVD) database holds 21,957 vulnerabilities published in 2021. This value is higher than in previous years (18,362 in 2020, 17,382 in 2019, and 17,252 in 2018). The National Vulnerability Database of the US government, which is supplied by the Common Vulnerabilities and Exposures (CVE) list, now includes over 150,000 entries.

For security researchers, the increase in attacks on critical infrastructure is a wake-up call. It revealed weaknesses by third-party companies, security experts, and outside agencies such as universities. Security researchers have been concerned about industrial control system (ICS) vulnerabilities stemming from high-profile hacking attacks on critical infrastructure. Therefore, further research into ICS vulnerabilities can help organizations better understand and manage cyber risks to critical infrastructure.

To address growing cyber risks, industrial companies need to make rapid and visible cybersecurity improvements to their operational technology (OT) and industrial control systems (ICS). The **i4Q Security Guidelines (i4Q^{SG})** aims to help in this ongoing and not stopping task.

1.1 Overview

With the increase in external threats, protection concepts are becoming increasingly important. Operators of critical infrastructure must maintain basic IT security standards and defend their systems from cyber-attacks. Effective protection concepts require a combination of organizational and technical measures, including at the very least a robust password policy, backup copies, updated systems, limited exposure to online services, and device encryption. To deploy holistic protection solutions, product vendors, system integrators, and operators must collaborate.

A standards-based strategy has many benefits, reducing the chances of a successful cyberattack, using a consistent set of standards across stakeholders, security across the lifecycle, and reducing overall lifecycle costs. Considering this, the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have joined forces to address the need to improve cybersecurity in Industrial Automation and Control Systems (IACS). The ISA/IEC 62443 series was developed and published by the ISA99 Committee and IEC Technical Committee 65/Working Group 10.

1.2 Introduction to IEC 62443 Standard

ISA-IEC 62443 [3] aims to improve the safety, reliability, integrity, and security of IACS using a risk-based, rigorous and comprehensive process throughout its lifecycle. The ISA/IEC 62443 Series specifies a set of terms and conditions that facility owners, product suppliers, and service providers must adhere to protect Control Systems and Equipment Under Control (EUC).

IEC 62443 lays out a road map for enterprises to follow in order to attain best-in-class performance through process improvements. There are five degrees of maturity according to the Software Engineering Institute's CMMI for Services (CMMI-SVC) concept.:

- 1-Initial: without a well-documented and properly regulated process
- 2-Managed: has a formalized method, evidence of skill, and properly educated staff
- 3-Defined: at maturity level 2 and demonstrates the use of defined, established and documented process as well as defined training schemas for personnel
- 4&5-Improving: at maturity level 3 as well as demonstration of continuous improvement

Progressing at each level will result in improved performance at the organizational level. Service providers and asset manufacturers must determine the maturity level associated with each requirement's implementation. Customers may see how strong an organization's cybersecurity policies and practices are by looking at the maturity levels.

1.2.1 Scope and Purpose

The ISA/IEC 62443 Series is concerned with the security of industrial automation and control systems. An IACS is a group of people, hardware, software, and laws that are engaged in the running of an industrial process that can affect or influence its safety, security, and reliability [4].

It's worth noting that an IACS encompasses more than just the technology that makes up a control system: it also encompasses the people and work processes required to maintain the control system's safety, integrity, reliability, and security. If an IACS lacks appropriately qualified employees, risk-appropriate technologies and remedies, and operational procedures all across security lifecycle, it may be more exposed to cyberattacks [4].

Because IACS are Cyber-Physical Systems (CPS), a hack might have serious consequences. A cyberattack on an IACS can have a variety of implications, among them, but not exclusively:

- Endangering the safety or health of the public or employees
- Environmental damage
- Equipment damage
- Product integrity is compromised
- A deterioration in public opinion or the company's reputation
- Failure to comply with legal or regulatory standards
- Information that is proprietary or confidential is lost
- Financial damage
- Consequences for entity, local, state, and national security [4]

The first four repercussions listed above are specific to physical-cyber systems and are not encountered in most ordinary IT systems. Indeed, it is this distinction that necessitates various techniques to safeguarding physical-cyber systems, prompting standards development bodies to recognise the need for IACS-specific standards. Other features of IACS that aren't seen in most IT systems include [4]:

- failure modes that are more predictable
- increased unpredictability and time-criticality

- higher availability
- a more strict approach to management
- extended durations of time between servicing
- Component lives are much longer
- Safety, Integrity, Availability, and Confidentiality (SIAC) in place of Confidentiality, Integrity, and Availability (CIA)

Cyber threat actors include insiders (accidental or intentional), hacktivists, cybercriminals, organized crime, and state-sponsored attacks, to name a few [4]. Ransomware, harmful software, specific remote access attacks, and organized attacks on control systems and related infrastructure are all examples of cyberattacks.

1.2.2 Design principle: Secure by Design

Secure by design is a design approach that necessitates the implementation of security mechanisms early in the IACS' lifecycle. Early in the development process, solid security policies, security architectures, and secure practices should be established and implemented [4]. This design concept can be used in product development as well as the production of automated solutions. Security features are built into the Control System or Component from the start when utilizing a secure by design philosophy, therefore no compensatory countermeasures are required.

1.2.3 Design principle: Reduce Attack Surface

Reducing the attack surface of IACS is a design technique that reduces the number of structural and logical interfaces that can be inspected and exploited, making a successful attack more difficult. To reduce the attack surface, design principles such as attack surface reduction are used:

- Access control: Access to IACS systems and networks is restricted both physically and logically
- Network segmentation: IACS networks can be segmented and traffic between them can be controlled
- Least function: eliminating superfluous functionality from IACS systems and networks to make them more secure
- Minimum privilege: restricting privileges to those that are absolutely necessary for the work.

1.2.4 Design principle: Defense in Depth

The layered use of various security measures to delay or avoid attacks is called defence-in-depth (DiD). DiD includes multiple layers of protection and detection, even on a single system, and requires attackers to breach or bypass multiple layers without being detected. Even though vulnerability is exploited in one layer, IACS is still secure. Special care should be taken when a single vulnerability allows many layers to be compromised potentially.

1.2.5 Design principle: Essential Functions

Crucial functions are functions or capabilities that are required to maintain the health, safety, environment, and availability of the Equipment Under Control. Some of the most critical functions are:

- Safety Instrumented Function (SIF)
- control function
- the operator's capacity to see and manage the Equipment Under Control

The loss of critical functions is known as "loss of protection," "loss of control," and "loss of view" [4]. Additional services, such as history, may be considered necessary in some instances. The concept of vital functions constrains the design of IACS security mechanisms in the following ways:

- Access control must not obstruct the performance of critical functions.
- If the border layer protection (firewall) enters in failure mode or island state, vital functions must be maintained.
- Safety instrumented functions will continue to function if a denial-of-service incident occurs on the control system network.

Next paragraphs will expand the basic aspect that IEC 62443 points as essential.

1.3 Introduction to ISO 27001 standard

It is the standard of information security. It specifies the requirements necessary to establish, implement, maintain and improve an information security management system. The main objectives of this standard are to preserve the confidentiality, integrity and availability of the system.

When implementing an Information Security Management System (ISMS) according to ISO 27001, it is important to consider Risk Assessment. The first step to implement this standard is to choose an appropriate risk assessment methodology [5].

1.3.1 Risk assessment methodology

There are numerous standardized risk assessment methodologies, but the following one is the methodology suggested in the Standard:

1. Identify the information assets and those responsible for them, i.e. everything that has value for the organization, such as physical supports, intellectual supports, informative supports, the brand, reputation etc. Moreover, it is necessary to identify the vulnerabilities of each asset those weaknesses of the asset that make it susceptible to attack or damage.
2. Identify the threats, there are the ones that can happen and damage the information asset.
3. Identify the legal and contractual requirements that the organization is obliged to comply.

4. Identify the risks that are defined for each asset, the probability that threats or vulnerabilities specific to the asset may cause total or partial damage to the information asset, in relation to its availability, confidentiality and integrity.
5. Risk calculation, which is based on the probability of occurrence of the risk and the impact it has on the organization, to determine the risks that must be controlled with priority.
6. Finally, the risk treatment plan must be defined the risk treatment policy based on the previous points and the policy defined by the management. At this point, it is where we will select the appropriate controls for each risk, which will be oriented to assume, reduce, eliminate, and transfer risk.

1.3.2 Benefits of applying ISO 27001

Information security risks represent a considerable threat to businesses due to the possibility of financial loss or damage, loss of essential network services, or loss of customer reputation and trust. This standard will help organizations better manage their information security risks.

Risk management is one of the critical elements in preventing online fraud, identity theft, damage, loss of personal data, etc. Organizations are exposed to many IT threats if they do not have a solid risk management framework.

An information security management system systematically manages sensitive company information to remain secure.

Moreover, the design and implementation of it will give confidence to customers and suppliers that information security is taken seriously within the organization, being at the forefront in applying technical processes to address information threats and security issues [5].

1.4 Security strategies

Growing security requirements result from increased networking and the use of proven IT environment technologies in automation systems. It is insufficient to provide simply a superficial and restricted level of protection, because external attacks might occur on multiple levels. For maximum protection, a thorough understanding of security and how to implement it is essential.

1.4.1 Motivation

Maintaining control over the production process is the first objective in automation. Measures aimed at reducing security risks must not obstruct this priority. Only authenticated users should be able to perform (authorized) operations, with access limited to those operation options permitted for usage by the authenticated user. The activity must be carried out solely through well-defined access channels to ensure that the production process continues to run smoothly throughout a command, with no risks to people, the environment, the product, the items to be coordinated, or the company's operations.

1.4.2 Strategies

A protection concept is comprised of general defence techniques that are meant to resist the following attacks, based on these claims [6]:

- availability reduction by means of denial of service.
- circumventing a security mechanism by means of man in the middle.
- authorized users performing wrong operations on purpose by means of stealing passwords.
- Inappropriate operations owing to user rights that have been misconfigured.
- unlawful data monitoring (such as commercial secrets and recipes, or the operation of machinery and systems, as well as their security procedures).
- modify data altering alarm levels.
- deleting log data files to hide attacks.

Traditional perimeter-based IT security models, designed to restrict access to trusted company networks, are unsuitable for the digital world. Companies today create and deploy applications in corporate data centers, private clouds, cloud environments (AWS, Azure, GCP, and others), as well as through SaaS solutions (Microsoft 365, Google Workspace, Box, etc.). Most businesses are expanding their defence-in-depth strategies to protect cloud workloads and defend against new offensive vectors that come with digital transformation.

As a result, many businesses are adopting an "assume-breach" mentality and adjusting their security strategies, relying on a conjunction of preventative controls and detection mechanisms to identify attackers and protect them from achieving their objectives once they have gained network access. The fundamental tenets of a modern DiD strategy.

1.4.3 Defense in Depth

Although the term Defense in Depth has been introduced before in section 1.2.4 more in-depth knowledge is provided by the following [7].

Defense in Depth is a data security technique in which a slew of security mechanisms and controls are purposefully stacked throughout a computer network to safeguard the network's confidentiality, integrity, and availability, as well as the data contained within it.

- Protect privileged access – Access to privileged accounts should be monitored and secured (superuser accounts, local and domain administrator accounts, application administrative accounts, and so on) privileged access management systems are used by both human and non-human identities (applications, scripts, bots, etc.).
- Lockdown critical endpoints – Deploy comprehensive endpoint privilege management systems to disable privilege across all endpoints, restrict lateral movement, and protect against ransomware and other types of malware.
- Enable adaptive multifactor authentication – Use context data (location, time of day, IP address, device type, etc.) and business rules to determine which authentication elements to apply to a specific user in a specific situation.
- Secure developer tools – Employ secrets management systems and other credentials used by apps, automation scripts, and other non-human identities to safeguard, manage,



rotate, and monitor secrets, such as 'HashiCorp Vault' or 'AWS Secrets Manager' or 'Knox' or 'Microsoft Azure key Vault' as examples.

The DiD idea includes layered security and recognition features that are more effective than stand-alone systems in terms of security. It has the following characteristics:

- Ability to detect attackers attempting to penetrate or circumvent the Defense in Depth structure.
- Defensive techniques in other layers can temporarily compensate for a weakness in one layer of this design.
- System security has its own layer structure inside the larger tiered framework of network security.

To secure on-premises IT assets, most businesses have built DiD plans around traditional perimeter-based security approaches. A traditional defence-in-depth security configuration includes a number of security components, such as [7]:

- Endpoint security – endpoint privilege management solutions, antivirus software, and endpoint detection and response (EDR) tools are used to protect against threats that originate on PCs, MACs, servers, and mobile devices.
- Patch management – to maintain endpoint operating systems and apps, as well as to mitigate common vulnerabilities and exposures (CVEs).
- Network security solutions – firewalls, VPNs, VLANs, etc. to protect traditional enterprise networks and conventional on-premises IT systems.
- Intrusion detection/prevention (IDS/IPS) tools – to detect suspicious activity and defend traditional on-premises IT infrastructure against cyber-attacks
- User identity and access management solutions – use single sign-on, multi-factor authentication, and lifecycle management solutions to authenticate and authorize users.

1.5 Industrial security vs Functional safety

The term “functional safety” refers to the safeguarding of the controlled environment against the system’s anomalous activities. Security, on the other hand, is concerned with the protection of a system’s regular operation against purposeful or unintentional infractions. Safety systems, on the other hand, must be particularly secured from such transgressions.

It is the responsibility of the machine vendor to provide appropriate safety procedures. Even if they can help, these mechanisms should not be incorporated in the defense in depth idea.

Security threats, unlike safety concerns, are dynamic throughout the life of an equipment or plant. As a result, security protection must be updated on a regular basis.

1.6 IT security vs Industrial security

In general, the security features built into PCs and Windows operating systems give a high protection level. These actions, on the other hand, are usually tailored to the needs of office environments. The items to be safeguarded in industrial security are relatively similar, although their priorities differ dramatically to some extent. While the confidentiality and integrity of

information are often the top goals in office IT, plant availability or operability is the top priority in industrial security. When choosing proper security actions, make sure they give the required protection level without taking an undesirable influence on the real operation.

1.7 Security Administration

Security administration is an important component of an industrial security strategy since it addresses all security-related aspects of an automation system, whether it's a single machine, a plant area, or the full plant. Security management, a procedure for monitoring and detecting these risks, should be considered as the potential pitfalls to an automated solution develop over time. This procedure aims to develop and maintain the required security level for an automated system throughout time. The risk analysis component of a security management process ensures that only the most suitable remedies are utilized to mitigate risks.

A plant's security measures must be examined and realigned on a regular basis, as mentioned before in the introduction of the IEC62443 standard.

- Risk assessment, including the development of countermeasures aimed at lowering the risk to a manageable level.
- Coordinated organizational and technical measures
- Repetition on a regular and event-driven basis

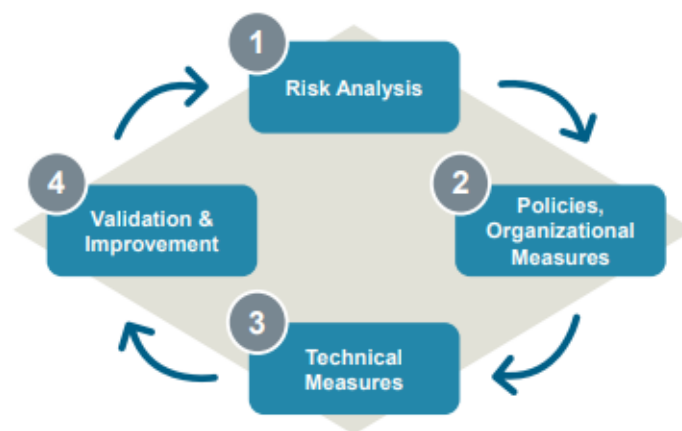


Figure 1. Security Management Process Cycle [8]

1.8 Public/Private Certificates

One main problem in electronics computing communication is the impossibility to verify that the sender of the communication is really who it claims to be. For example, in the world to verify the identity of a person, documents such as the passport are used accompanied by a signature or a photograph that identifies to the person. To duplicate this process using digital technologies, certificates are employed. As a result, a digital certificate is a digital document that proves the identifying entity's ownership of the public key contained within it (person,



device, or computer). This is approved by a Certification Authority (CA) and guarantees that the CA has validated and trusted the entity to which the certificate belongs.

Digital certificates allow verifying that the other party with whom it is established the connection is who it claims to be. The robustness of the certificates lies in their generation process on, which makes use of public key cryptography. This not only allows you to check the identity of the device, but the device will be able to sign your data before sending it, thus ensuring the confidentiality and integrity of everything you send. As increases the number of devices, also increases the life cycle management problems of the certificates in use.

2 Technical Specifications – Application

In this section, it will be described how the previously showed theory and recommendations are translated to the real world.

2.1 Installing a feeling of accountability

Only if all parties involved cooperate responsibly the security strategy can be implemented successfully into solutions in automation systems. This includes the following:

- Include the development also system tests and security tests to manufacturers
- Include planning, structuring, and factory acceptance test to systems integrators
- Include operational and administrative task to owner and machine operators.

Throughout the system's entire service life, the strategies and their implementation must be monitored and revised just from the initial offer submission, continuing with planning and design, to finalize with system migration and uninstallation.

The features listed below do it possible for an automation system's protection concept to be effective:

- usage of high availability, tested products with hardened and well-defined security settings that are specifically built for industrial applications.
- a modern configuration that uses cutting-edge technology and standards to create a system that is tailored to the customer's security requirements.
- operating systems and components with care and responsibility in accordance with the manufacturer's intended uses.

2.2 Layered protection

The following factors are included in this strategy's multi-layer security paradigm [8]:

- Risk analysis
- Plant Security
 - i. Physical access protection
 - ii. Processes and guidelines
- Network security
 - i. Perimeter network
 - ii. Firewalls and VPN
- System integrity
 - i. System hardening
 - ii. Authentication and access protection
 - iii. Patch Management
 - iv. Detection of attacks

The benefit of this method is that an attacker must first break through multiple security layers before being able to inflict any damage. Each layer's security requirements can be taken into account separately.

2.2.1 Risk analysis

The first step in determining security actions is to do a risk analysis. Risk analysis is a necessary pre-requisite for Security Management of a production environment or device, as it identifies and assesses specific dangers. A risk analysis' content typically contains the following:

- Identification of threatened objects
- Determination of current security measures
- Assessing the possibility for damage and determining the worth
- Threat and weak points analysis
- Risk assessment

Compensating measures must be used to eliminate or lessen the recognized and unacceptable risks. On the other hand, the risks that are eventually acceptable can only be determined for each application individually. However, no one safeguard, nor a combination of measures, can ensure complete security.

2.2.2 Plant Security

The foundation for developing and implementing an industrial security solution is the implementation of an adequate, comprehensive security management system.

Security management is mostly made up of four steps:

- Risk analysis and reduction actions: Based on the hazards and risks assessed, these actions must be established for the plant.
- Establishing standards and coordinating executive actions.
- Technical measures must be coordinated.
- A security management approach that repeats risk assessments on a regular or event-based basis.

To maintain a standard approach and uphold the Industrial Security concept, policies and practices must be created [8]:

Security-related policies examples:

- Requirements for adequate safety risks that are consistent
- Methods to report events and strange acts
- Communication and documenting of security incidents
- In the production area, the use of mobile PCs and data storage like prohibiting their usage outside of the fabrication area
- Guidelines for product, solution, or service providers

Examples of Security relevant processes:

- Dealing with known/corrected flaws in used components
- Procedure to follow in the event of a security breach
- Procedure for resuming production after a security breach
- Security events and configuration changes are recorded and evaluated
- Procedure for testing and checking multiple data devices prior to their use in the manufacturing line

To establish a unified approach and uphold the Industrial Security concept, physical access shield of essential production facilities must be determined:

- Procedures to avoid illegal entry to the plant
- Differentiated access authorizations and physical separation of distinct production zones
- Physical access control for automation components that are critical (e.g., control cabinets that are secured)
- Physical security and plant IT security guidelines must be synchronized.

Physical access concerns may arise as a result of a lack of countermeasures:

- Unauthorized access to production facilities / buildings
- Physical damage to or replacement of manufacturing equipment
- Espionage results in the loss of confidential information.

Risks associated with company security may be avoided by the use of the following measures:

- The company's premises are fenced in and monitored
- Logging, locks, ID card readers are all examples of access controls
- Visitors and outside personnel are guided by company personnel.

Measures to reduce the danger of physical production security include:

- Access to restricted manufacturing locations is limited
- Critical components, such as surveillance and alarm facilities, in securely lockable control cubicles / rooms

2.2.2.1 Security check list

They are intended for standalone IPCs that do not have access to the internet. The solution should be adapted to the corresponding operating system or running environment.

2.2.3 Network Security

If a network segment contains PLC or other smart objects that have no or limited self-protection, the network segment is considered vulnerable, establishing a secure network environment for these devices is a wise option to consider. The usage of network security appliances is one way to accomplish this. Individual sub-networks can be segmented for added security, using a demilitarized zone (DMZ).

Continuous communication from the control room to the field is more critical than ever, as evidenced by contemporary developments like digital twins and industrial IoT. Complete connectivity, on the other hand, poses increased degrees of risk, it necessitates the implementation of security measures:

2.2.3.1 Separation between production and office networks

The separation of production networks from other company networks is the initial step in network segmentation. In the most basic situation, separation is done by a unique firewall that regulates or restricts communication between the networks. Link is established over a separate DMZ network in the more secure option. Firewalls prevent direct contact between the

production and business networks; communication is only possible indirectly through those servers in the DMZ network.

2.2.3.2 Cell protection concept

Component protection against unauthorized access and network overload, and other risks by segmenting the production network into numerous secured automation system cells:

- A network section is safeguarded from external illegal access using the cell protection concept.
- Data flow within a cell is not managed by a Security Appliance and is judged safe or strengthened by cell-level security measures.
- A unit comprises only elements that must be protected in the same way.
- The network structure should be determined by the manufacturing process. Enabling it to define lower cells with minimum firewall approvals and less communication across cell borders.
- Encrypted VPN connections to the PLC can be established directly.

2.2.3.3 Secured remote control for service and maintenance

Permission requires authentication, which enables for the secure validation of the subject's identity. Following the completion of the authentication procedure, permission policies are implemented. The authorization procedure determines what data you have access to.

- Maintaining and operating an onsite server for secure remote access
- Granular user and group administration allows for device-independent access control
- Fine-grained user permissions, full audit capability, and ISO 27001 certification [5].

2.2.3.4 Secured connection to cloud solutions

The security of data transport and access control must be ensured:

- For device access and data transfer, TLS communication methods are suggested.
- Instead of anonymous access, passwords or certificates should be used to authenticate devices and data access.
- Existing network division and cell defence concepts, such as firewalls or network separation, should be preserved.

2.2.3.5 Security check list

A number of dangers and their solutions are listed in the following checklist [18]. These notes are additional proposals for IPCs with network connection to the previously explained in the section 2.2.2.1. Again, this security checklist only shows the recommended settings, the solution should be adapted to the corresponding operating system or running environment.

2.2.3.6 Specific firewall for users

Using specific rules to control the access can prevent the access of unknow users to the system. Additionally, these rules can also control the access that each user has to each part of the system.

2.2.3.7 Security monitoring

This concept is related with monitoring the suspicious behaviour of the system. With this monitoring some alerts can be triggered depending on the behaviour of the system. The early detection of suspicious or unnormal behaviour will help improving the security of the system.

2.2.4 System Integrity

It is critical to limit vulnerabilities in IT systems and at ICS in order to ensure system integrity. The following solutions could be used to achieve this need:

- antivirus and whitelisted software should be used
- patch administration
- authentication for plant and machine workers
- Access control techniques included into IACS
- program code protection by know-how security, copy safeguards, and password assignment

2.2.4.1 Access protection for configuration

Using the inbuilt access protection methods to avoid unauthorized configuration modifications is highly recommended. This comprises, for instance:

- For user authentication using firewalls
- For user authentication using WLAN access points
- For user authentication using managed switches
- For access protection for device settings using HMI panels
- For protection levels for configuration and HMI access using PLCs
- For know-how protection using drives

Related with passwords, use a variety of passwords that are both secure and unique. At least 12 characters in upper and lower case, numbers, and special characters. A password manager is also recommended for easy password management. This one should be saved on a centralized network point with access privileges in case of coordination among multiple people.

2.2.4.2 Access protection for runtime operations

Because the machinery in a plant is typically managed by multiple people, it is advised that user administration is centralized. This is based e.g. on user accounts in a Windows domain or Windows Active Directory. A unified user administration makes it easier to check access authorizations on a regular basis (e.g., identifying unused accounts) and to set and enforce security policies (e.g., validity of passwords, monitoring of erroneous loggings, etc). It's also worth noting that user accounts should be limited to the bare minimum of operational rights, based on the required responsibilities (operator, administrator, etc.).

2.2.4.3 Access protection for network components (Network)

There should be systems in place to secure networks from unauthorized access:

- Using switch ports, to restrict access by means of MAC or IP access lists
- Device administration and RADIUS authentication by means of 802.1X
- Network perimeter security in respect to other networks using firewalls

Mechanisms for WLAN security should be established by the use of:

- Data exchange security in compliance with at minimum WPA2
- Encoding data with Advanced Encryption Standard (AES)
- RADIUS authentication (802.1x) for Central device administration
- HTTPS web interface and SSH sessions provide secure configuration access

2.2.4.4 System hardening

System hardening reduces possible attack scenarios and, in that sense, next a short list is shown with some well-known or common-sense rules to follow when configuring or system hardening [8]:

A. Related to: Network Services

Active network services, in general, are a security risk. Only the services that are truly required on automation components should be activated to reduce dangers. In the security concept, all activated services (particularly Webserver, FTP, Remote Desktop, and so on) should be considered. Hardening measures (network robustness) in automation and driving goods are an excellent practice that improve security without requiring additional user settings.

B. Related to: HW and System Interfaces

If illegal access to equipment or the system is feasible through hardware interfaces, they pose a threat. As a result, unused interfaces should be turned off:

- USB, Ethernet and PROFINET ports.
- WLAN, Bluetooth and Mobile Communications.

Blocking mechanism and deactivation procedures should be used to safeguard interfaces. Booting and autostart mechanisms should be disabled depending on the hardware or external media (USB devices). In this regard, like with hard disks, BIOS access protection as well as UEFI settings should be enabled. And any remote access, such as AMT (Active Management Technology), should be done securely.

C. Related to: User Accounts

It should be remembered that every active user account with access to the system, is a security thread. As a result, user accounts must be limited, setup, and activated to the bare minimum. For existing accounts, strive to use secured access data whenever possible. Accounts, particularly locally configured user accounts, should be audited on a regular basis in order to have documentation of who, what, and when traces occur.

When it comes to strengthening user accounts, it's also crucial to remember that if specified default passwords exist, they must be changed during system commissioning.

Previously in sections 2.2.2.1 and 2.2.3.5 had been showed some actions to follow in order to avoid weaknesses, in other words, following those recommendations of the tables we do 'system hardening'.

2.2.4.5 Updates and patch management

Patching and updating software are crucial steps towards improving security. And the sooner is patched a system the better security is achieved. Many modern security attacks take advantage of flaws for which manufacturers have already released remedies. When a vulnerability isn't yet discovered or fixes aren't available, it's called a zero-day exploit.

Because manual patch management is inefficient and prone to failure, setting up update groups, redundant systems, and processes for online patch delivery streamlines patch. The updating procedure is simplified by having a central patch server in the DMZ with Windows Server Update Services (WSUS) installed. Next in section 2.5 detailed information is given regarding the update or patching programs procedure.

As soon as vulnerability is discovered, it should be evaluated to see if it applies to the application involved. On the basis of this, it can be decided whether or not more actions should be taken:

- Since existing safeguards are enough no action is required
- Extra external security actions to maintain the security level
- Installing the most recent firmware upgrades to fix the flaw

To detect malware and prevent it from spreading further, antivirus software should be utilized. Certain considerations should, nevertheless, be considered depending on the circumstances:

- Decreased performance because of the scan method: during maintenance times
- Regular update of virus patterns: if applicable via centralized server

It should be noted that, even if a system is infected with malware, availability must be guaranteed. This means that the virus scanner must not be used in any way:

- Delete files, restrict access to them, or place them in quarantine.
- Block communication
- Shutdown systems

2.2.4.6 Whitelist

Whitelisting procedures are a fundamental principle for both preventing unwanted applications or viruses and detecting illegal changes in installed applications. Whitelisting software generates or maintains a list of applications and apps that are permitted to run on the computer, and anything not on the list is not. In a whitelisted environment, there are no frequent or delayed pattern updates, as there are in other automatic out-of-the-box systems.

2.3 Public Key Infrastructure

A valid and reliable critical distribution infrastructure is required to allow public keys on a network such as the Internet. A Public Key Infrastructure (PKI) enables a company to use advanced technology such as digital signatures, cryptography, and digital certificates to provide electronic authentication systems with confidentiality, data integrity, and non-repudiation for their network applications.

Digital signature technology, based on public key cryptography, is used in public key infrastructure. The fundamental premise is that each entity's secret key is known only to that entity and is used to sign documents. This key is referred to as the private key. It generates a public key that is used to validate signatures but cannot be used to sign anything. This public key is normally contained in the certificate document and is made available to everybody. PKI provides trust services, this requires trusting the actions or outputs of things, whether people or computers. One or more of the following capabilities are respected by trust service objectives: Confidentiality, Integrity and Authenticity (CIA).

- Confidentiality: Encrypting data streams and messages protects the privacy of user transactions. The secrecy function may be used to prevent unwanted information disclosure on a local or network level. Users can ensure that only the intended recipient can “unlock” (decrypt) an encrypted message by utilizing PKI.
- Integrity: Another key role of PKI is to ensure message integrity. PKI contains built-in checks to ensure that all outputs are the same as the inputs. Any tampering with the data can be identified and avoided instantly. It is often less important to prevent integrity from being compromised (tamper proof), but it is critical that if integrity is compromised, there is unambiguous evidence of the compromise (tamper evident).
- Authenticity: The process of validating that the user is who they claim they are is known as authentication. The (PKI) allows senders and recipients to verify each other's identities.
- Non-Repudiation: PKI assures that an author cannot deny signing or encrypting a communication after it has been transmitted, as long as the private key is kept secure. Digital signatures serve as a link between sender's and their messages. All communications signed with the sender's private key were transmitted by that specific person because only the message's sender can sign messages with their private key.

2.3.1 Basic functions of the PKI

The operations carried out by a PKI can be very diverse, but the most important are:

- 1) Issue, renew and revoke a certificate.
- 2) Create, review and revoke a key.
- 3) Check the status of a certificate.
- 4) Carry out management and administration operations.
- 5) Store certificates in a reminder list.
- 6) Publication of keys: once the keys are created, the PKI allows us to disseminate our public key, as well as locating the public keys of other users, along with their status (key revoked...).

One of the advantages of PKI is that it does not depend on any specific technology, but that provides a framework of action on which to work, according to the needs in each particular case.

2.3.2 i4Q chain of trust

In order to fulfil i4Q communication security needs, there had been identified the next aspects to create a PKI infrastructure:

- Creation of a root_CA: this will be the Certificate Authority (CA) feed to create, identify and link the all the entities associated to the project.
- Creation of sub_CA: Depending on the needs and the number of the partners involved in the project, one sub_CA will be created for each organization. In this way each company or organization will be independent from the others in order to control and maintain its PKI and related certificate structure.
- Creation of dedicated sub_CA: focused on the functionality and the type of the needed certificate, different subCA will be created. Dedicated subCAs will be used, as for example, one subCA to create certificates used in SSL/TLS communications, other subCA to create certificates to use for authenticating communications in cloud services, etc.

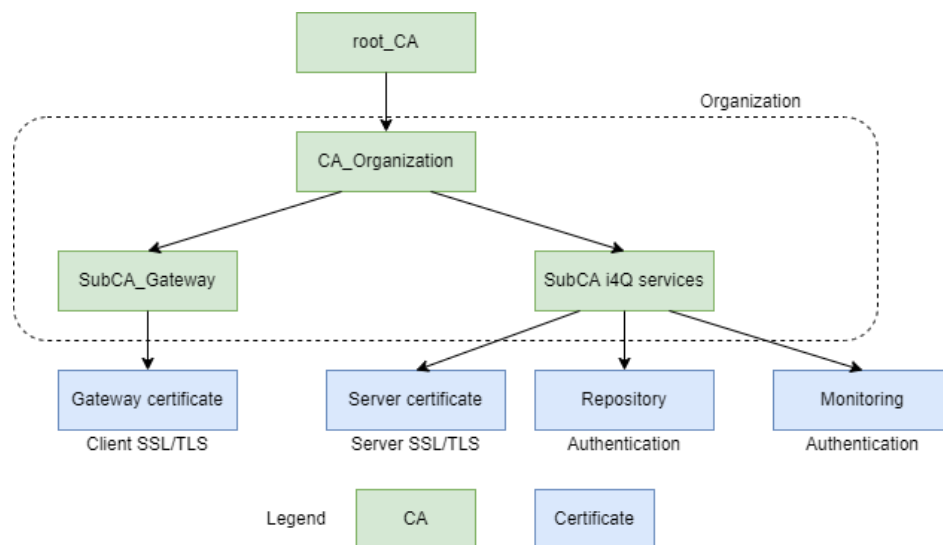


Figure 2. i4Q PKI structure proposal

- Flexible structure: As shown in the previous **Figure 2**, the proposed three level CA structure is flexible enough to grow as needed to fulfil actual and future needs as well as it is adaptable to the requirements of the different companies involved in Up2Date.

2.3.3 Certificate Management

Certificate management systems are software tools that allow us to carry out all essential PKI operations. Basically, they usually allow validating the requests they receive, issue certificates, process OCSP queries, create and distribute CRL, store keys and manage tokens (these last two, could be done using a dedicated hardware device called HSM). In addition, it is also common (as well as necessary) that allow maintenance and administration of the PKI, such as managing the roles of the administrators, consult the log, create and delete CA, VA, RA, among others.

There are numerous options available for ready-made certificate management systems to work. Many of them are open source like “Lamassu IoT”[, others only have a paid version such as “Windows Server”, “Digicert” or “Entrust”, and some have a basic free version like “EJBCA”[or “Vault”[that can be upgraded with a payment version (which usually includes support).

2.4 Validation and Improvement

A Security Audit should be undertaken after all planned steps have been implemented to ensure that (1) the measures have been implemented as planned, and (2) the identified risks have been reduced as predicted. Measures can be altered and/or added based on the results in order to achieve the required level of security.

Due to changes in security threats and specific occurrences, it is necessary to repeat the risk analysis on a regular basis to ensure the security of plant/machinery.

2.5 Updates/Patches in ICS

Running firmware and/or application program patches or updates in ICS, with antivirus as an additional program, may require special attention to address security vulnerabilities [10].

The phrase “[antivirus]” refers to anti-malware software that protects against not only viruses but also other types of harmful software. When properly implemented and kept up to date, AV is a crucial aspect of a defense-in-depth approach for protecting against malicious and malware software in ICS.

Each antivirus client in most IT systems is configured to receive updates directly from the antivirus provider or from the organization’s servers, which are located in a secure subnet within the company network and receive updates from the antivirus or equivalent provider.

The ICS system should be isolated from other networks, such as IT networks, to maintain separation and isolation. This makes it more difficult to keep software up to date, necessitating other methods of updating it [10].

2.5.1 Considerations

It is impossible to overestimate the necessity of confirming the update and its source, as well as testing updates. Automatic updates usually lack any means of integrity verification aside from the program’s cyclic redundancy check (CRC) or the communication protocol. The cryptographic hash of the update provides additional confidence that the file has not been tampered with. Although an attacker might break into an antivirus or firmware manufacturer’s website and change the update file as well as the cryptographic hash value, the attacker would have to put in more effort, and the vendor would most likely identify and block the attempt. This could influence your antivirus software selection. Asset owners should make sure they can manually update their assets.

Antivirus software is an important aspect of an organization’s supply chain, despite popular belief []. Because either one could be an attack vector, all software and firmware should be evaluated as part of the product evaluation. Before adding vendors and their goods to an approved products list, an organization should ideally have a program in place to analyse them and make ensuring they satisfy operational and security requirements. Here are several examples such as, the FIPS 201 Evaluation Program [12], GSA IT Schedule 70 [13], and the Department of Defense Information Network Approved Products List (DODIN APL) [14]. A product evaluation program’s specific criteria and process should be tailored to the organization’s needs and capabilities.

Furthermore, a number of "next-generation" firewalls and intrusion prevention systems can analyze traffic and prevent malware from infecting endpoints by preventing it from transiting a network. This, however, must be a device capability that has been configured.

2.5.2 Software Update strategies

Secure network design recommendation for ICS [10], **Figure 3**, places the antivirus, Windows Server Update Services, and patch server(s) in a layered DMZ. These programs (AV/WSUS/patch) should be hosted on their own hosts if at all possible, and not in a single server hosting three separate applications either physical or virtual. Traffic to each host should be restricted following the hardening recommendations explained before in section 2.2.4.4. Each level in this subnet design should only send or receive traffic to a level directly nearby to it. This prevents the AV/WSUS/patch server from talking directly with either provider antivirus servers, which are typically situated outside the corporate network, or corporate antivirus servers, which are typically located within it.

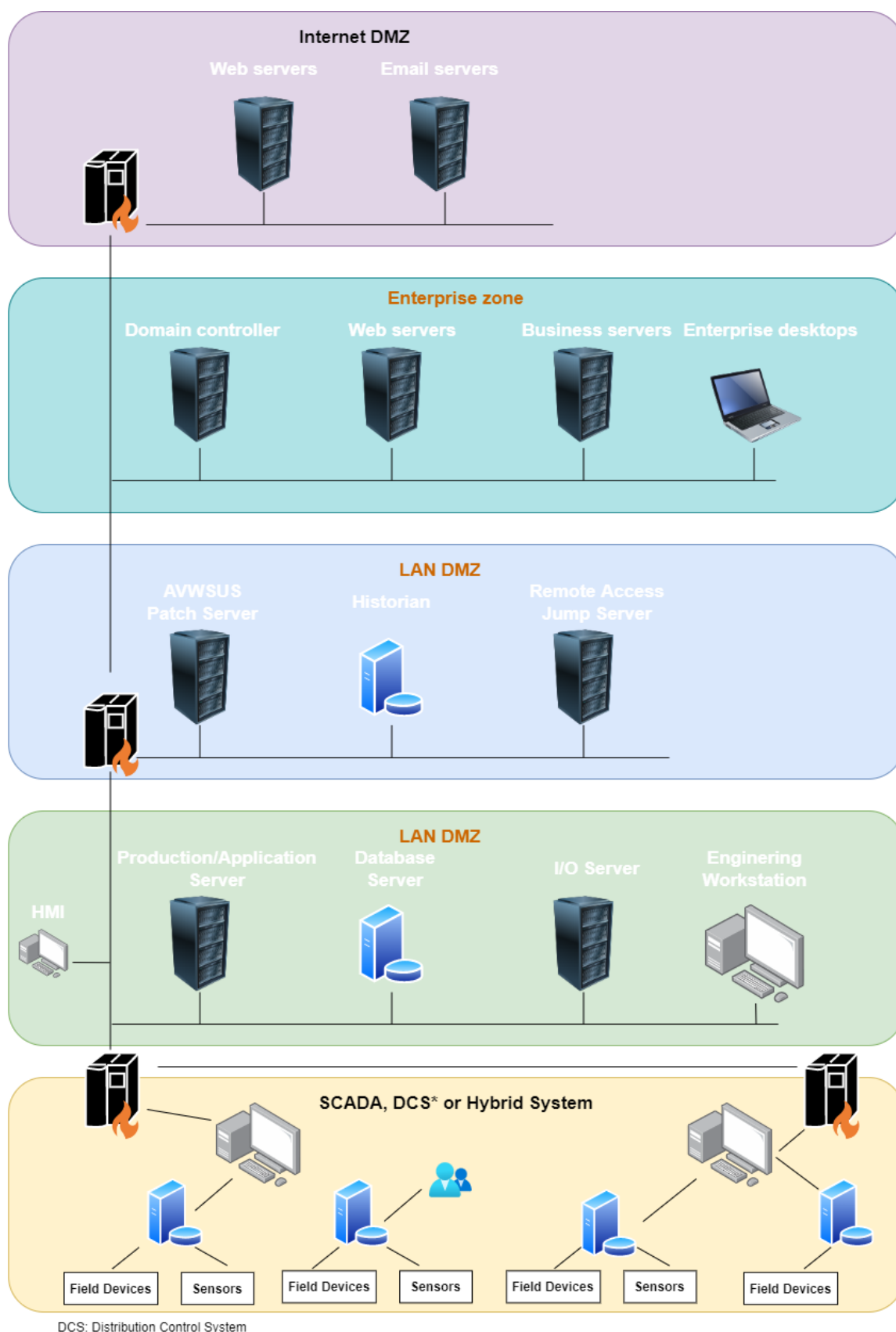


Figure 3. Layered network architecture

The antivirus update procedure is complicated by restricting data transfer only to adjacent zones, hence a better solution is necessary. Updates are downloaded from provider antivirus

servers to a specialized host and written to removable media, then updating the AV/WSUS/patch server using that media is one method. Although this strategy appears to be time-consuming at first appearance, it is not. If the asset owner employs this strategy, it is critical to take care to avoid introducing malware or otherwise jeopardizing the ICS. This would entail ensuring that the update source is valid, that the hash values of the updates are proper, and that employees handle distribution media safely. Employees should also observe the company's external storage policy and other standards when managing media, according to asset owners.

The processes for transmitting updates in this manner are as follows:

- 1) Confirm the update's source.
- 2) Back up the update files to a separate server.
- 3) Run a virus scan on the downloaded file.
- 4) Verify the cryptographic hash of each file.
- 5) Set aside one media for updates alone, and scan it for viruses or other unusual data before using it to ensure its integrity.
- 6) If feasible, lock the media so that no one else can write to it.
- 7) Place the media in the test environment and make sure it has no negative effects on the test system.
- 8) Verify that the update has no negative impact on the production system by testing it on a non-critical endpoint or system segment.
- 9) Update the remaining hosts with the patch.
- 10) Finally, check the system for any unexpected behaviour and make sure the ICS is working properly.

This method, named as 'sneaker net'[is normal in separated or layered networks. While this method necessitates extra effort than automatic update binding, it does not take an enormous amount of time.

Another option is to have the updates automatically 'daisy chained.' The update server in the LAN-DMZ of the control centre gets its updates automatically from some other server in the corporate area, and gets its patches from the antivirus dealer's servers.

2.5.3 Test and Validation

Regardless of the setup, testing is necessary because there is always the chance of an inconsistency or restriction having an adverse effect on the system. Before changing any production endpoint, it's also a good idea to back it up (if possible). If the update has a negative impact, having a backup will make it easier and faster to recover. As part of the overall change management program, asset owners should document the distribution and testing of upgrades. This should be a well-defined procedure with workers in charge of keeping it up to date.

Testing is essential because updates can have a negative impact on ICS setups; there have been instances where ICS apps have malfunctioned as a result of antivirus software installation or upgrades. Antivirus scanning can drastically augment CPU and RAM consumption, interfering with applications and processes on devices with insufficient resources. One of the reasons why it's necessary to maintain test environments that closely mimic production environments is because of this. Updates should be installed first on a test system, and the system's proper



operation should be checked for any negative consequences or odd behaviour. If no problems arise, distribute the upgrade to operative systems in the following order: IT network, ICS DMZ second, and ICS network third. Update non-critical assets first in each operating system, as any negative impact is less likely to impact or otherwise damage processes.

The goal of software updates and upgrades is to make sure a better level of security. An increased level of security makes results in decreasing downtime and other negative repercussions of an ICS. The technique should be customized to the environment in order to meet the organization's operational and security demands, however, it should always include updates verification, level separation to enable DiD, and testing for every update.

3 Implementation Status

3.0 Current implementation

Due to the nature of this deliverable, as it is a guideline to apply in ICS systems in order to improve security, it is not applicable to measure the implementation level.

3.1 History

Version	Release date	New features
V0.1	26/02/2022	Update/upgrade and patching in ICS
V0.2	01/03/2022	ICS network architecture
V0.3	10/03/2022	Risk management and cybersecurity governance
V0.4	15/03/2022	ICS Network perimeter security
V0.5	24/03/2022	Host security description
V0.6	02/04/2022	Physical security description
V0.7	07/04/2022	defence-in-deep description
V0.8	20/04/2022	Public Key Infrastructure
V0.9	26/04/2022	IEC 62443 Series of Standards
V0.10	02/05/2022	Security strategies
V0.11	12/05/2022	Conclusions. Ready to internal review.
V1.1	07/11/2022	Some information is added to complete Section 2
V1.2	01/12/2022	Sections 2.2.3.6 and 2.2.3.7 have been completed. And a section about ISO 27001 has been added.
V1.3	19/12/2022	Images updated
V1.4	30/12/2022	Final version

Table 1. i4Q^{SG} Version history

4 Conclusions

The **i4Q Security Guidelines** (i4Q^{SG}) highlighted relevant aspects of cybersecurity in ICS, describing best practices and relevant aspects to defend against an ever-expanding list of cyber-related threats. Significant ISO 27001 and IEC 62443 standards have been presented, and it has been stated that a four-phase cyclical process that contains (1) Risk Analysis, (2) Comprehensive security management and policy setting, (3) Technical Measures, and (4) Validation and Improvement is essential [19].

A special section has been dedicated to the update, upgrade, and patches strategy, as well as the defence-in-depth approach as a strategy to protect against cyber-related threats [19].

The use of a public key infrastructure is proposed to ensure trust between the elements of the ICS ecosystem by providing confidentiality, integrity, and authenticity among them via X509 certificates [19].



References

- [1] Kaspersky ICS CERT. <https://ics-cert.kaspersky.com/publications/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019>
- [2] <https://www.comparitech.com/blog/information-security/cybersecurity-vulnerabilitystatistics>
- [3] https://en.wikipedia.org/wiki/IEC_62443
- [4] NIST SP 800-82 REVISION 2, Guide to Industrial Control Systems (ICS) Security
- [5] https://es.wikipedia.org/wiki/ISO/IEC_27001
- [6] www.cyberark.com. <https://www.cyberark.com/resources/blog/five-tools-for-a-defence-in-depth-strategy-for-endpoints>
- [7] www.cyberark.com. <https://www.cyberark.com/es/what-is/defence-in-depth/>
- [8] Siemens. <https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf>
- [9] Lamassu IoT. A PKI for the Internet of Things (IoT). <https://www.lamassu.io/>
- [10] EJBCA. Open Source PKI Software. <https://www.ejbca.org/>
- [11] Vault. Identity-based security. <https://www.vaultproject.io/>
- [12] FIPS. <https://www.idmanagement.gov/sell/fipsannouncements/>
- [13] GSA IT Schedule. <https://www.igov.com/gsa-schedule-70.htm>
- [14] DoDIN approved list. <https://aplits.disa.mil/processAPList.action>
- [15] Sneakernet. <https://en.wikipedia.org/wiki/Sneakernet>
- [16] www.cisa.gov. <https://www.cisa.gov/tips/st04-006>
- [17] https://www.cisa.gov/uscrt/sites/default/files/recommended_practices/Recommended%20Practice%20Updating%20Antivirus%20in%20an%20Industrial%20Control%20System_S508C.pdf
- [18] Siemens https://cache.industry.siemens.com/dl/files/014/109475014_/att_970828/v3/109475014_Security_settings_IPCs_Win10_en.pdf
- [19] i4Q Cybersecurity Guidelines. [Online]. Available: https://i4q.upv.es/5_i4Q_CSG/index.html



Appendix I

https://i4q.upv.es/5_i4Q_CSG/index.html **i4Q Cybersecurity Guidelines v2** (i4Q^{SG}) web documentation can be accessed online at: https://i4q.upv.es/5_i4Q_CSG/index.html