D3.5 – i4Q Cybersecurity Guidelines

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	D3.5 – i4Q Cybersecurity Guidelines			
WORK PACKAGE	WP3 – BUILD: Manufacturing Data Quality			
DATE OF DELIVERY	CONTRACTUAL	June 2022	ACTUAL	June 2022
NATURE	Report	DISSEMINATION LEVEL	Public	
LEAD BENEFICIARY	IKERLAN			
RESPONSIBLE AUTHOR	Aitor Uribarren (IKER)			
CONTRIBUTIONS FROM	10-TUB, 20-BIESSE			
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. A second version will be provided namely “D3.13 i4Q Cybersecurity Guidelines v2”.			
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 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	12-May-2022	ToC	ToC created and sent for review	IKER
0.2	10-Jun-2022	Working Version	1st input to all sections	IKER
0.3	17-Jun-2022	1st Draft	First draft sent for internal review	IKER
0.4	20-Jun-2022	Internal review	Internal review	TUB, BIESSE
0.5	24-Jun-2022	2nd Draft	Addressing the comments from the internal review. Updated draft sent to the coordinator.	IKER
1.0	30-Jun-2022	Final doc	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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

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
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DiD	Defense in Depth
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
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
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
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
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
SIAC	Safety, Integrity, Availability, and Confidentiality
SIF	Safety Instrumented Function
SSH	Secure Shell
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** (i4Q^{SG}) Solution providing the general description and technical application.

The phrase "industrial control system" (ICS) encompasses a broad range of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other system control topologies such as programmable logic controllers (PLC), which are commonly used in industrial and critical infrastructure applications.

Increased attacks on any infrastructure served as a wake-up call for security researchers to pay more attention to ICS flaws. As a result, additional research into ICS vulnerabilities could help organizations better identify and handle the cyber dangers that critical infrastructure faces.

This guideline intends to highlight important parts of ICS cybersecurity by presenting best practices and significant aspects for defending against an ever-growing list of cyber-related threats.

Document structure

Section 1: Contains a general description of the **i4Q Security Guidelines** (i4Q^{SG}), providing an overview and the list of main design principle's. 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 administers 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 is a higher number 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 fed by the Common Vulnerabilities and Exposures (CVE) list, now includes over 150,000 entries.

For security researchers, the increased attacks on key infrastructure served as a wake-up call. External entities such as third-party companies, security experts, and academia, among others, disclose vulnerabilities. Security researchers have been focusing on Industrial Control System (ICS) vulnerabilities as a result of high-profile hacks against vital infrastructure. As a result, additional research into ICS vulnerabilities may be able to help enterprises better identify and handle the cyber risks that critical infrastructure faces.

To fight against a growing range of cyber-related risks, industrial enterprises need rapid and demonstrable improvements in their Operational Technology (OT) and Industrial Control Systems (ICS) cyber security. 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 a number of benefits, a decreased chance of a successful cyberattacks, the use of a consistent set of criteria among stakeholders, security throughout the lifecycle, and the overall lifespan costs is lower. In this sense, The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have joined forces to address the need to improve the cybersecurity of Industrial Automation and Control Systems (IACS). The ISA99 Committee and the IEC Technical Committee 65/Working Group 10 develop and publish the ISA/IEC 62443 Series.

1.2 Introduction to IEC 62443 Standard

The objective of the ISA-IEC 62443 [3] is using a risk-based, rigorous, and comprehensive procedure throughout the lifetime, increase the safety, reliability, integrity, and security of IACS. The ISA/IEC 62443 Series establishes a collection of terms and conditions that must be followed by asset owners, product suppliers, and service providers to safeguard 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.

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.

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

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 stricter 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. 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. 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 an IACS's attack surface is a design technique that reduces the number of structural and logical interfaces that can be probed and exploited, enabling an attack more difficult to succeed. Design principles such as reducing the attack surface are used to reduce the assault surface:

- 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 deployment of various security measures, in layers, with the purpose to postpone or avoid an attack is known as Defense-in-Depth (DiD). Even on single systems, defense in depth involves numerous layers of protection and detection, and requires attackers to break through or bypass multiple layers without being detected. Even if a vulnerability in one layer is exploited, the IACS remains secure. Extra caution is required when a single vulnerability allows for the probable compromising of many levels.

1.2.5 Design principle: Essential Functions

Essential functions are functions or capabilities that are essential to sustain the Equipment Under Control's health, safety, the environment, and availability. Among the most important functions are:

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

The loss of important functions is referred to as "loss of protection," "loss of control," and "loss of view". 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 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.

1.3.1 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.

1.3.2 Strategies

A protection concept is comprised of general defense techniques that are meant to resist the following attacks, based on these claims [5]:

- availability reduction be 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, which were designed to limit access to trusted company networks, aren't well adapted for the digital world. Businesses today create and deploy applications in corporate data centers, private clouds, and public clouds (AWS, Azure, GCP, and others), as well as using SaaS solutions (Microsoft 365, Google Workspace, Box, etc.). To safeguard cloud workloads and defend against new attack vectors that come with digital transformation, most firms are expanding their defense-in-depth tactics.

As a result, many businesses are adopting a Zero Trust "assume-breach" mentality and adapting their security strategies, relying on a combination of preventative controls and detection mechanisms to identify attackers and prevent them from achieving their objectives once they have gained access to a network. A modern DiD strategy's key tenets.

1.3.3 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 [6].

Defense in Depth is a data security technique in which a multitude of security mechanisms and controls are purposefully piled throughout a computer network to protect the network's confidentiality, integrity, and availability, as well as the data housed inside 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 – To lock down privilege across all endpoints, limit lateral movement, and guard against ransomware and other kinds of malware, deploy comprehensive endpoint privilege management systems.
- Enable adaptive multifactor authentication – To identify which authentication elements to apply to a certain user in a specific situation, leverage contextual information (location, time of day, IP address, device kind, etc.) and business rules.
- Secure developer tools – To safeguard, manage, rotate, and monitor secrets, use secrets management systems and other credentials used by apps, automation scripts, and other non-human identities, 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.

Most firms nowadays have built DiD plans around traditional perimeter-based security approaches to secure on-premises IT assets. A traditional defense-in-depth security setup includes a variety of security components, like:

- Endpoint security: Control access to privileged endpoint accounts with endpoint privilege management solutions; antivirus software and endpoint detection and response (EDR) tools to protect threats originated from PCs, Macs, servers, and mobile devices.
- Patch management: to keep endpoint operating systems and apps up to date, 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 activities and protect traditional on-premises IT infrastructure from cyber-attacks.
- User identity and access management solutions – To authenticate and authorize users, employ single sign-on, multi-factor authentication, and lifecycle management solutions.

1.4 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.

1.5 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.

1.6 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

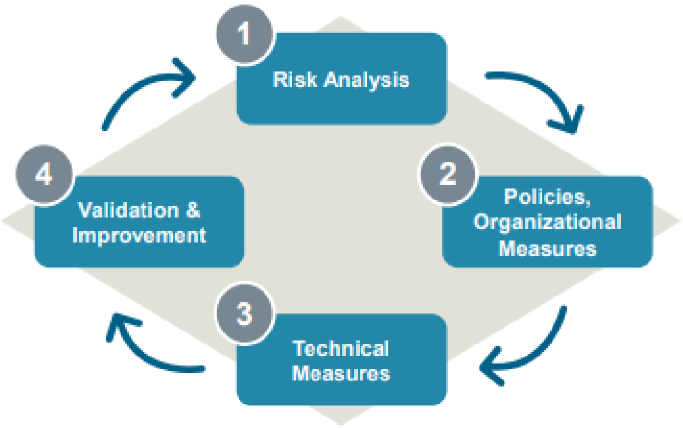

Figure 1. Security Management Process Cycle [7]

1.7 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 confirms that the public key contained inside it belongs to the identifying entity (person, device, or computer). This is issued by a Certification Authority (CA) and ensures that the identification of the entity to which the certificate belongs has been validated and trusted by the CA.

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 can the security strategy be successfully implemented 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 administrational 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:

- 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' typical 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 [7]:

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

The check list in page 5 of the next work **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**] identifies a number of threats and their solutions. 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 an 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

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 defense 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 check list [17] in page 6. These notes are additional proposals for IPCs with network connection to the previously explained in the section 2.2.2.1. Again, these security check list only shows the recommended settings, the solution should be adapted to the corresponding operating system or running environment.

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 [7] 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 be centralized. This is based on user accounts in a Windows domain or Windows Active Directory, for example. 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, ...). 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 minimun 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 know or common sense rules to follow when configuring or system hardening[7]:

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 is a crucial step 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 a 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 preventing unwanted applications or viruses, as well as to detect illegal changes in installed applications. Whitelisting software creates or keeps track of a list of applications and apps that are allowed to operate on the computer, and anything that isn't on the list isn't. There are no frequent or delayed pattern updates in a whitelisted environment, as there are in other automatic out-of-the-box systems.

2.3 Public Key Infrastructure

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

A public key infrastructure makes use of digital signature technology, which is based on public key cryptography. 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 senders 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 regarding 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, ...

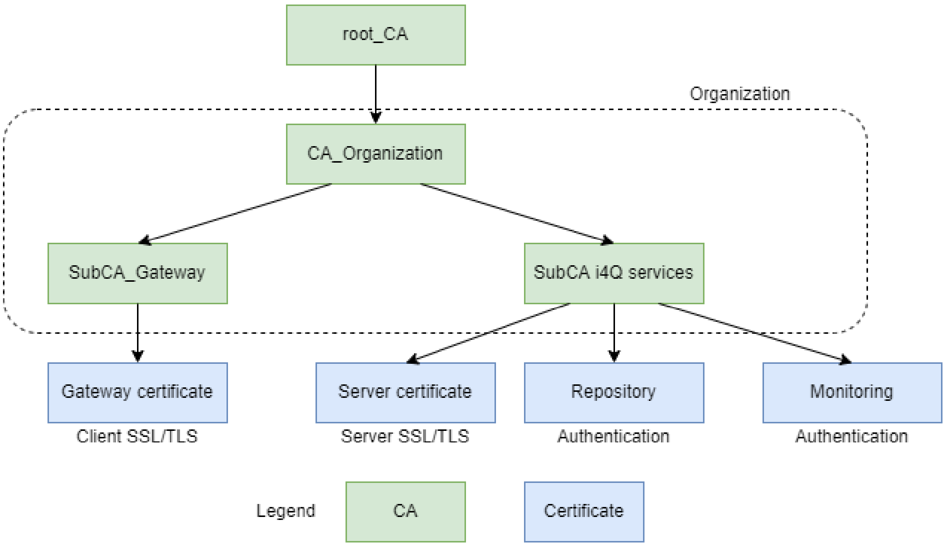

Figure 2. i4Q PKI structure proposal

- 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 very 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” [8], others only have a paid version such as “Windows Server”, “Digicert” or “Entrust”, and some have a basic free version like “EJBCA” [9] or “Vault” [10] 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, antivirus included as another program, may require special attention to fix security vulnerabilities [16].

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.

In most IT systems, each antivirus client is set up 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 separated from other networks such as IT ones maintaining separation and providing isolation between both networks. This makes more complicated to keep software up to date requiring other strategies to updating it.

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 [15]. 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 [11[11], GSA IT Schedule 70 [12], and the Department of Defense Information Network Approved Products List (DODIN APL) [13]. 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 [16],

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.

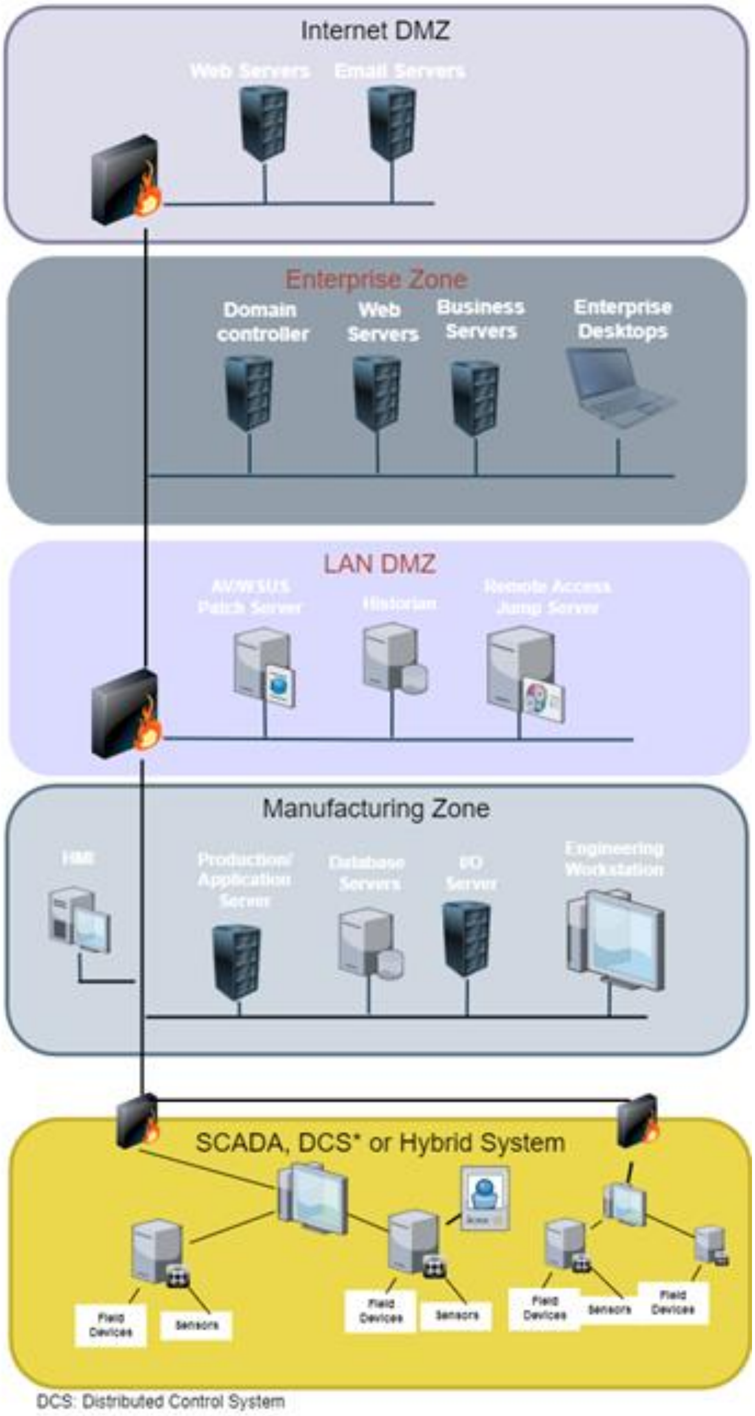

Figure 3. Layered network architecture

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’ [14] 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

3.1 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.

3.2 Next developments

If applicable, in M24 updated and corrected final version.

3.3 History

Version	Release date	New features
V0.0.1	26/02/2022	Update/upgrade and patching in ICS
V0.0.2	01/03/2022	ICS network architecture
V0.0.3	10/03/2022	Risk management and cybersecurity governance
V0.0.4	15/03/2022	ICS Network perimeter security
V0.0.5	24/03/2022	Host security description
V0.0.6	02/04/2022	Physical security description
V0.0.7	07/04/2022	defense-in-deep description
V0.0.8	20/04/2022	Public Key Infrastructure
V0.0.9	26/04/2022	IEC 62443 Series of Standards
V0.0.10	02/05/2022	Security strategies
V0.0.11	12/05/2022	Conclusions. Ready to internal review.

Table 1. i4Q^{SG} Version history

4. Conclusions

The **i4Q Security Guidelines** (i4Q^{SG}) emphasized relevant aspects regarding cybersecurity in ICS, describing good practices and relevant aspects to defend against a growing list of cyber-related threats. Relevant ISO 27001 and IEC 62443 standards have been introduced and there had been concluded that it is crucial to conduit a four-phase cyclical process that includes (1) Risk Analysis, (2) Comprehensive security management and policy setting, (3) Technical Measures, and (4) Validation and Improvement.

Special relevance has been given to the update, upgrade and patches strategy with a specific section, as well as to the defense-in-deep approach as strategy to protect cyber-related threats.

The usage of a public key infrastructure is proposed in order to guarantee trust between the elements in the ICS ecosystem providing confidentiality, integrity and authenticity among them by means of X509 certificates.

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-vulnerability-statistics.

[3] https://en.wikipedia.org/wiki/IEC_62443

[4] NIST SP 800-82 REVISION 2, Guide to Industrial Control Systems (ICS) Security

[5] www.cyberark.com. https://www.cyberark.com/resources/blog/five-tools-for-a-defense-in-depth-strategy-for-endpoints

[6] www.cyberark.com. https://www.cyberark.com/es/what-is/defense-in-depth/

[7] Siemens. https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf

[8] Lamassu IoT. A PKI for the Internet of Things (IoT). https://www.lamassu.io/

[9] EJBCA. Open Source PKI Software. https://www.ejbca.org/

[10] Vault. Identity-based security. https://www.vaultproject.io/

[11] FIPS. https://www.idmanagement.gov/sell/fipsannouncements/

[12] GSA IT Schedule. https://www.igov.com/gsa-schedule-70.htm

[13] DoDIN approved list. https://aplits.disa.mil/processAPList.action

[14] Sneakernet. https://en.wikipedia.org/wiki/Sneakernet

[15] www.cisa.gov. https://www.cisa.gov/tips/st04-006

[16]https://www.cisa.gov/uscert/sites/default/files/recommended_practices/Recommended%20Practice%20Updating%20Antivirus%20in%20an%20Industrial%20Control%20System_S508C.pdf

[17] Siemens https://cache.industry.siemens.com/dl/files/014/109475014 /att_970828/v3/ 109475014_Security_settings_IPCs_Win10_en.pdf

Appendix I

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

i4Q Cybersecurity Guidelines (i4Q^{SG})

General Description

This solution is a guide to achieve data reliability and quality in a manufacturing line by enough cybersecurity mechanisms to ensure some level of security in industrial environments. For security researchers, the increased attacks on key infrastructure served as a wake-up call. External entities such as third-party companies, security experts, and academia, among others, disclose vulnerabilities. Security researchers have been focusing on Industrial Control System (ICS) vulnerabilities as a result of high-profile hacks against vital infrastructure. As a result, additional research into ICS vulnerabilities may be able to help enterprises better identify and handle the cyber risks that critical infrastructure faces.

Relevant ISO 27001 and IEC 62443 standards are introduced and there had been concluded that it is crucial to conduit a four-phase cyclical process that includes (1) Risk Analysis, (2) Comprehensive security management and policy setting, (3) Technical Measures, and (4) Validation and Improvement.

Special relevance has been given to the update, upgrade and patches strategy with a specific section, as well as to the defense-in-deep approach as strategy to protect cyber-related threats.

The usage of a public key infrastructure is proposed in order to guarantee trust between the elements in the ICS ecosystem providing confidentiality, integrity and authenticity among them by means of X509 certificates.

Features

The main aspects considered in i4Q^{SG} are as follows:

1. **Secure by Design**: is a design approach that requires security measures to be introduced early in the IACS' lifespan. The goal is to establish strong security policies, security architectures, and secure practices early in the development process and implement them throughout the lifespan.
2. **Reduce Attack Surface**: is a design method that lowers the amount of physical and functional interfaces that can be accessed and exploited, making an assault more difficult to succeed.
3. **Defense in Depth**: The deployment of various security measures, especially in layers, with the purpose to delay or prevent an attack is known as Defense-in-Depth (DiD). Even on single systems, defense in depth implies numerous layers of protection and detection, and requires attackers to break through or bypass multiple layers without being detected.
4. **Essential Functions**: are defined as functions or capabilities that are essential to sustain the Equipment Under Control's health, safety, the environment, and availability of the Equipment Under Control that include Safety Instrumented Function, the control function, and the ability of the operator to view and manipulate the Equipment Under Control

5. **Public Key Infrastructure**: a digital certificate is a digital document that confirms that the public key contained inside it belongs to the identifying entity (person, device, or computer). This is issued by a Certification Authority (CA) and ensures that the identification of the entity to which the certificate belongs has been validated and trusted by the CA. A Public Key Infrastructure (PKI) allows a company to have electronic authentication systems with confidentiality, data integrity and non-repudiation for their network applications.
6. **Updates/Patches in ICS**: The ICS system should be separated from other networks such as IT ones maintaining separation and providing isolation between both networks. This makes more complicated to keep software up to date requiring other strategies to updating it. Running firmware and/or application software patches or upgrades under ICS, with antivirus as a separate program, may necessitate extra care to avoid security risks.

Commercial Information

Authors

Company	Website	Logo
IKERLAN	www.ikerlan.es/en/	ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Associated i4Q Solutions

Required

None. Due to the nature of the document, it is expected that it will be serve as reference in the implementation of security mechanisms by the rest of the i4Q solutions.

Optional

None.