IoT/OT SECURITY

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

June 10, 2025

Code: PO-IT-I&C-SEC016

prysmian

The planet's pathways

TABLE OF CONTENTS

1. PURPOSE & OBJECTIVE

The purpose of this document is to provide guidance for securing Operational Technology (OT) systems and Internet of Things (IoT) devices, including Industrial Control Systems (ICS) and the supporting organizational and technological infrastructure, in order to reduce the Information Security risks arisen from the integration, coordination and management of IT and IoT/OT solutions.

This Policy is based upon the standards set by ISO 27001 series, NIST Cyber Security Framework and the applicable laws and regulations, including – but not limited to – the General Data Protection Regulation (GDPR)

2. POLICY OWNER

Information & Cyber Security Function owns this Policy and is responsible for periodically reviewing and updating it to ensure it accurately reflects organizational updates or legal and regulatory changes.

3. APPLICABILITY

This policy is intended for all the personnel, internal and external, that use and manage systems within the Group's production environment, including employees, suppliers, partners and contractors.

4. YOUR RESPONSIBILITY AS EMPLOYEE

This Policy requires you to:

a) Read, understand, and comply with the requirements included in this Policy;
b) Comply with Prysmian's Code of Ethics and any other applicable policies or procedures;

c) Report immediately to the appropriate channels outlined in Section 6 of the **Helpline Policy** any alleged violation of this Policy, both if committed by a Prysmian employee or an external stakeholder;
d) Ask questions or report any concerns related to this Policy;
e) Complete assigned training related to this Policy when required.

5. GENERAL PRINCIPLES

Nowadays, industrial environments are the main fields of an ever-increasing integration between OT, IoT and IT solutions, helping companies to automate, optimize and make "smart" all the phases of industrial operations. While ICSs are migrating from physically and logically isolated systems, running proprietary control protocols and using specialized hardware and software, to distributed architectures, adopting IT solutions, standard applications and network protocols, IoT devices are becoming more and more employed within industrial processes and used to promote corporate business systems connectivity and remote access capabilities. The several benefits arising from IT, IoT and OT interconnection, firsts of all the reduction of operational costs and the increase of performance, have rapidly promoted this evolution, leading ICSs to increasingly resemble IT systems and IoT devices to be more pervasive within the production sites.

Besides the benefits mentioned above, the "new" Industrial Environment could be exposed to several Information Security threats and risks. Considering that OT and IoT systems are typically employed within critical production processes, any interruption or disruption of their functionality could result in human safety and environmental damages, beside the financial, reputational and operational damages.

Due to operational requirements of plants and factories (e.g. systems should operate 24/7 and cannot be shut down, systems are more likely to be repaired that replaced, communication protocols could be old and unsecure, etc.), Information Security risks posing on Industrial Environment cannot be addressed through classical security techniques and best practices employed within non-industrial environments. Thus, in addition to classical

and standard Information Security measures, companies should apply new ones, properly tailored for OT and IoT environment.

5.1. IoT/OT Security Governance

The IoT/OT Security Governance domain comprises strategy and organizational aspects of the secure management of IoT/OT systems and technologies, including the associated roles and responsibilities, the risk management process, the defined policies and processes, the supply chain and compliance aspects and the Information Security training and awareness activities.

IoT/OT Security Governance activities must be carried out in accordance with the following general principles.

- IoT/OT Security roles and responsibilities should be defined and assigned to selected personnel. IoT/OT Security responsible should manage the Information Security measures to be applied to the production systems, coordinating IT and OT Departments efforts, and monitor the Information Security threats posing on the IoT and OT environment.
- IoT/OT Security risks should be identified, monitored, evaluated and managed following a structured Risk Management approach and considering the peculiarities of the IoT and OT environment. IoT/OT Security Risk Management process, including its evaluations and actions, should be aligned with the corporate, safety and environmental aspects.
- A specific set of IoT/OT Security policies, procedures and operating instructions should be defined, formalized, periodically updated and approved by management. IoT/OT Security documents should be made available to interested parties (employees, ICS operators, relevant external parties, maintenance personnel, etc.).
- Applicable international and local regulations affecting the Industrial Environment should be identified. Regulations requirements should be evaluated and implemented on the affected IoT/OT systems. Applicable local and international privacy regulations, e.g. the General Data Protection Regulation (GDPR), should be considered in order to identify and apply privacy requirements for IoT systems.

- IoT/OT Security risks associated with supplier's access to the organization's assets should be managed by means of specific measures and agreements. All relevant supply chain IoT/OT Security requirements should be established, agreed with each supplier and documented. Vendors and service providers for Industrial Environment should be selected based on security assessments and evaluations that take into account the criticality of business information, systems and processes involved.
- Specific trainings and awareness initiatives related to IoT/OT Security topics (e.g. IoT/OT Security trends and vulnerabilities, update of policies and procedures, IoT/OT Security measures and best practices to be adopted) should be defined and regularly provided to ICS personnel and other internal and external interested parties.

5.2. Information Protection

The Information Protection domain is related to the secure and proper management of Group Information, during all the phases of the lifecycle, from creation to disposal, including classification scheme and encryption needs.

Information Protection activities must be carried out in accordance with the following general principles.

- Information should be classified based on a classification model that considers level of sensitivity of information and the impact of a potential unauthorized disclosure or modification. An Information classification process should be defined and implemented in accordance with the information classification scheme adopted by the Organization.
- Confidentiality, authenticity and integrity of information should be protected by employing proper cryptographic measures. Encryption algorithms should be selected considering the classification level of information, the results of a risk analysis and the operational requirements.
- Information should be protected during its whole lifecycle, from creation to disposal. Appropriate security measures should be implemented to protect assets containing sensitive information. Formal procedures should be defined in order to regulate and manage the proper disposal and sanitization of assets.

5.3. Identity and Access Management

The Identity & Access Management domain comprises organizational aspects and technical controls regarding the identification, authentication and authorization of IoT/OT systems users, considering the whole lifecycle of the identities and accounts, from creation to deletion or change.

Identity & Access Management activities must be carried out in accordance with the following general principles.

- Logical access to IoT/OT systems should be controlled and reviewed with a structured process. Users should be uniquely identified and authenticated on the systems prior giving them access to the information stored and its functionalities in order to prevent unauthorized activities. Identification and authentication mechanisms should be enforced.
- Roles, rights and permissions on the IoT/OT systems should be assigned to Group personnel according to the Identity and Access policy and to the least privilege principle. Separation of duties should be respected in order to properly disseminate tasks and associated privileges among multiple users.
- Identities and accounts should be managed with a structured process encompassing all the phases of their lifecycle, from the creation and activation to the modification and removal. Different profiles for ICS personnel should be defined and enforced on the IoT/OT systems (e.g. administrators, operators, guests, etc.).

5.4. Application Protection

The Application Protection domain is related to the secure and proper management of the software and application part of IoT/OT systems, including security design and testing.
Application Protection activities must be carried out in accordance with the following general principles.

- Information Security measures should be applied to software employed within IoT and OT environment, considering both application management aspects, such as

periodical penetration tests and code review, and application design aspects, such as input and output validation controls.

- Security-related activities should be included within the different phases of the Software Development Lifecycle, from the design of the solutions to the testing and deployment. Rules and guidelines for the secure development of applications should be established and applied to the software development activities of the Organization.

5.5. Network and Communication Protection

The Network and Communication Protection domain comprises the technical and operating aspects of the design and management of the data transmission channels and networks, including management and configuration of networking devices, confidentiality and integrity of the exchanged data and cloud security aspects.

Network and Communication Protection activities must be carried out in accordance with the following general principles.

-
- Authenticity, integrity and trustfulness of production data, devices and software should be guaranteed. IoT/OT data and networking devices should be monitored and controlled in order to detect any unauthorized modification.
- Network traffic and data flows to and from IoT/OT networks and systems should be restricted and controlled by applying secure architecture principles. Networks should be segregated according to a zoning model in order to allow only necessary system-to-system communication and prevent unauthorized access to IoT/OT network resources.
- Cloud services to be employed within Industrial Environment should be selected considering Information Security and operational requirements. Specific statements should be formalized within the agreements with cloud service providers in order to guarantee confidentiality, integrity, availability and authenticity of data, both in transit or stored within the cloud.

- Data exchange and communications within IoT/OT environment (to, from and between IoT and OT systems) should be performed by means of secure channels and protocols. A set of rules should be developed in order to monitor and control remote and local communications and limit the network access to the IoT/OT systems.

5.6. Physical and Environmental Security

The Physical & Environmental Security domain is related to the protection of Group facilities, production hardware and other physical assets.

Physical & Environmental Security activities must be carried out in accordance with the following general principles.

- Physical access to Group facilities should be monitored and controlled in order to prevent or detect any unauthorized access. Different security areas, with different levels of access and different physical security measures, should be defined considering criticality of structures, systems and data they contain. Physical access permissions and rights should be limited, regularly reviewed and role-based.
- Equipment and systems should be protected from intentional physical damages or natural hazards to ensure the continuity of the operations and the availability of information. Facilities and structures should be provided with mechanisms and sensors aimed at detecting, preventing and responding to environmental and structural threats.

5.7. IoT/OT System Protection

The IoT/OT System Protection domain comprises the organizational and operating aspects of the management of IoT/OT systems from a configuration / security baseline point of view.

IoT/OT System Protection activities must be carried out in accordance with the following general principles.

- Security configurations and controls baselines should be produced and maintained in order to implement or check the correct implementation of security measures on IoT/OT systems. The security baselines should be properly tailored to the different types of IoT/OT systems in order to address the peculiarities, architecture and security needs that each IoT/OT system could have. Specific controls should be defined for off-site IoT/OT assets, taking into account the risks of working outside organization's premises.
- Mechanisms and tools to prevent, detect, mitigate and protect the IoT/OT systems from the effects of malicious code and unauthorized software should be implemented and continuously maintained up to date.
- Risks introduced by the use of mobile devices should be managed defining and implementing a specific policy and supporting security measures. Security controls should be automatically enforced on portable and mobile devices.
- IoT/OT assets should be properly monitored and managed by means of a structured asset inventory. The asset inventory should be maintained and periodically reviewed, e.g. it should be updated upon deployment of new IoT/OT systems and assets and when changes occur in the IoT/OT environment. The asset inventory should contain information about the ownership and the criticality of the asset in order to better address potential security issues and monitor their resolution.
- IoT/OT systems architectures and functionalities should be designed considering all relevant security aspects and should be regularly tested under a security point of view in order to highlight potential design vulnerabilities. Hardening activities should be performed on IoT/OT systems according to their exposure and sensitivity, in order to reduce the risk of system to be compromised.
- For OT systems that cannot be updated or altered (e.g. legacy systems), compensating measures, such as network segregation, micro segmentation, system relocation or additional real-time monitoring activities, should be defined and applied.

5.8. IoT/OT System Acquisition and Maintenance

The IoT/OT System Acquisition and Maintenance domain comprises the organizational and technical measures to manage the OT Security aspects during the IoT/OT systems lifecycle,

from the acquisition and development to the disposal, including the maintenance activities needed to ensure an appropriate security level to the system operations.

System Acquisition and Maintenance activities must be carried out in accordance with the following general principles.

- Information Security aspects and principles should be taken into account during all the phases of the development lifecycle of the IoT/OT system, from the customization, purchasing and analysis of the solution to the testing and deployment, by adopting a security by design approach.
- Maintenance and repairs activities on IoT/OT system components should be managed according to the security best practices, to the manufacturer or vendor specifications and to the organizational requirements. All maintenance activities should be authorized and documented.
- A process to discover vulnerabilities that exist within IoT/OT systems, prevent their exploitation and timely mitigate them, leveraging automatic and manual tools, should be defined and implemented. Consideration on system adverse effects and possible production process disruption should be taken into account before using automatic solutions on IoT/OT environment. The criticality of assets and systems should be considered in order to prioritize the mitigation of security gaps.

5.9. IoT Devices Security

The IoT Devices Security domain is related to the specific aspects introduced by the adoption and management of IoT devices, smart and connected products within production facilities. IoT Devices Security activities must be carried out in accordance with the following general principles.

- Cybersecurity should be addressed considering the peculiarities of IoT devices, such as limited computing power and processing capabilities constraints. Cybersecurity in IoT systems should be embedded by introducing fail-safe and fail-secure mechanisms from design. IoT devices should be equipped with identification and authentication features.

- Secure/encrypted methods for admiration of IoT devices and communication between IoT devices and other connected systems should be implemented (e.g. HTTPS, SSH and associated key management).

5.10.Threat Management

The Threat Management domain is related to the analysis of, monitoring of and readiness testing against, the threat events that could impact the Group production facilities.

Threat Management activities must be carried out in accordance with the following general principles.

- IoT/OT Threat intelligence information should be collected and managed following a structured process in order to identify potential attack sources and types and new vulnerabilities which are relevant for the Group IoT/OT environment. A threat intelligence program could employ basic methods, such as following cyber security news, or advanced one, for example using of specific automatic tools.
- The readiness of the company response to a possible cyber-attack should be regularly tested and documented in order to determine the effectiveness and the adequacy of the responsive capability of the Group (e.g. table-top exercises, red teaming exercises).

5.11. IoT/OT Security Analytics

The IoT/OT Security Analytics domain comprises organizational and technical aspects related to the monitoring and performance evaluation of the IoT/OT systems.

IoT/OT Security Analytics activities must be carried out in accordance with the following general principles.

- Availability of IoT/OT resources and required system performance should be guaranteed analyzing and addressing the capacity requirements of IoT/OT systems, monitoring, measuring and tuning the usage of resources and making projections about future capacity needs of the IoT/OT technology.

- IoT/OT security events information and IoT/OT security logs should be produced, collected and periodically analyzed in order to ensure visibility into all aspects of organization's IoT/OT environment. Logs should contain information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, etc. Logs should be protected from unauthorized access, modification, and deletion. IoT/OT systems operators and administrators activity logs should be also produced and reviewed.
- IoT/OT system behavior and standard operations should be continuously monitored using commonly accepted security industry practices and recommendations in order to detect, characterize and report security events and anomalies in a timely manner.

5.12. Incident Management and Business Continuity

The Incident Management and Business Continuity domain comprises aspects related to the management of potential Information Security incidents and emergencies, including discovery, resolution, communication, and to the continuity of business processes and IoT/OT systems after a disruption.

Incident Management and Business Continuity activities must be carried out in accordance with the following general principles.

- Security incidents within the IoT/OT environment should be handled according to a structured process that encompasses all the phases of the incident management, from the reporting of the event though appropriate channels to the identification of affected assets, from the escalation to the closure. For each phase, roles and responsibilities should be established. The process should be updated upon internal and external context changes.
- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) should be developed, defining procedures to ensure the continuity of core processes and return to the normal and well-defined state of operations in case of disruptive events. Alternate storage sites, alternate processing sites and redundancies within the IoT/OT technological environment should be established.

- A comprehensive backup plan should be created and applied to the OT systems, considering the criticality of each system. Backups should be performed before updates and other important changes to the system. Physical and logical protection of backups, as well as the possibility to access them when needed, should be ensured.

6. CONSEQUENCES OF POLICY VIOLATION

As a Prysmian employee, you are agreeing to uphold our commitment to this Policy. Prysmian employees who violate this commitment or do not comply with this Policy shall be subject to disciplinary procedures, including possible dismissal, and any other legal action required to protect the interest and reputation of Prysmian, in line with the applicable legislation.

7. REPORTING A POLICY VIOLATION

All employees, contractors, and third-party users are required to report any suspected or actual violations of this Information Security Policy or any Security Incident immediately. All reports will be treated confidentially and investigated promptly. Ensuring the integrity and security of our information systems is a collective responsibility, and your cooperation is essential in maintaining a secure environment.

It is critical that potential violations are reported, internally, promptly as this may allow for immediate containment of any situation and prevention of an actual breach. Additionally, reporting is required to allow Prysmian to take the appropriate action, internally and externally, with regulatory reporting if it is required. Communication with the regulatory authority will be managed and coordinated by Corporate Affairs to protect the reputation and manage the liabilities of Prysmian.

As a Prysmian employee, you are required to report any Policy violation to:

a. **Cybersecurity@prysmian.com;** or
b. your Regional Compliance Team or the other designated subjects mentioned in Section 6.1 of the **Helpline Policy**.

Any form of retaliation, including threats and attempts of retaliation, is strictly prohibited. Prysmian is committed to ensuring that all employees are free to disclose any violation, either real or suspected, of the Prysmian's Company policy or procedure, to the extent they have reasonable grounds to believe that the matters reported are true. You will not be adversely impacted or retaliated upon in the workplace, either personally or professionally, for raising a valid and legitimate concern.

8. AUDIT, MONITORING AND CONTINUOUS IMPROVEMENT

The Owner of this Policy is responsible to perform periodic reviews and updates of this document, examining, in particular, revisions to be made based on internal organizational updates, changes to external legislation and best practices.

Using a risk-based approach, on a periodical basis the Information Security Function and the Internal Audit Department may perform, respectively, monitoring or audit activities aimed at verifying the correct enforcement of this Policy within the organization.

9. RELATED DOCUMENTS

The following Documents are related to this Policy and must be consulted by all Prysmian employees for further guidance. Part of such documents are available in the Ethics & Integrity Section of our Company's Intranet and are also publicly available within the correspondent Section of our Corporate website.

a) "Document and Record Management" document
b) "Information Security Strategy" document
c) "Information Security Policy" document
d) "Network Security Redesign Guidelines" document

APPENDIX A – DEFINITIONS

Availability – It is the capacity to ensure that Information is accessible and usable, when required, by authorized users, entities or processes.

Confidentiality - It is the capacity to prevent Information from being disclosed to unauthorized individuals, entities or processes.

Industrial Control System (ICS) – An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial Control Systems include Supervisory Control and Data Acquisition systems (SCADA) used to control geographically dispersed assets, as well as Distributed Control Systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information – Any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audio-visual.

Information Security – The protection of Information and information systems from unauthorized access, use disclosure, disruption, modification or destruction in order to guarantee confidentiality, integrity, and availability of Information.

Integrity – It is the capacity to protect Information from malicious or accidental modification or manipulation ensuring its accuracy and completeness.

Internet of Things (IoT) – A suite of technologies and applications embedded into devices with an increased capability of collecting, analyzing and managing information for instant data analysis and "smart" actions.

Operational Technology (OT) – The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of industrial equipment, assets, processes and events.

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Security Requirements – Requirements levied on an information system that are derived from applicable laws, contractual agreements, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability – The weakness of an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX B – DOCUMENT HISTORY

The history of changes is shown below. The most recent changes are listed first.

Version	Date	Major Changes
1	21/05/2021	First release
1.1	10/04/2022	Revision and Update
1.2	10/06/2025	Change template and revision