EUROPEAN CYBER SECURITY ORGANISATION

# System security and certification considerations

WG1 – Standardisation, certification and supply chain management

*December 2021*

# About ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional, and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

### ***Contact***

For queries in relation to this document, please contact wg1_secretariat@ecs-org.eu.
For media enquiries about this document, please contact media@ecs-org.eu.

### ***Disclaimer***



### ***Copyright Notice***

# Table of Contents

**About ECSO ..... i**

**1 Document scope and objective ..... 4**

1.1 Context ..... 4

1.2 Purpose ..... 4

1.3 Scope & objectives ..... 4

1.4 Intended audience ..... 4

1.5 Out of the scope ..... 5

**2 System security description ..... 6**

2.1 System definition ..... 6

2.2 Difference between system security and product security ..... 6

2.3 EU regulation security requirements ..... 7

**3 System security concerns ..... 8**

3.1 Security governance ..... 8

3.2 System security lifecycle and threat landscape evolution ..... 9

3.3 System stakeholders: roles and responsibilities ..... 10

3.4 Domain expertise ..... 11

3.5 Responsibility and cyber risk transfer between stakeholders ..... 12

3.6 Security architecture and design challenge ..... 12

3.7 Vulnerability and incident management challenge ..... 13

3.8 Cyber security interoperability ..... 13

**4 Certification considerations ..... 15**

**5 Conclusion ..... 18**

**6 Bibliography ..... 19**

**Annex 1 Glossary ..... 21**

**Annex 2 Examples ..... 25**

# 1 Document scope and objective

## 1.1 Context

This document is conceived based on common interpretation of the rich and diverse information available in International or EU standards, EU legislation and experience on system conception and deployment by ECSO Members.

## 1.2 Purpose

This document should serve as a high-level awareness document on the system lifecycle security and relevant certification information when applicable. This document aims to have a level of simplification that fits the majority of stakeholders, including non-system security experts.

## 1.3 Scope & objectives

This document aims to provide information and considerations to EU stakeholders on the particularities that make the cyber security of systems a special case and is meant to address any system type or size.

The document has the intention to describe the thinking process needed to conceive and secure systems during all phases of their lifecycle, highlighting the key cyber security actions needed and their relevant stakeholders.

This document will also describe the importance of a high-level risk assessment that defines a cyber security risk perimeter and provides important risk comprehension for all subsequent actions in a coherent framework.

This document will also cover important security notions of the systems' lifecycle related to governance, maturity and diversity of processes, products and people that can design, build, and ultimately run a mission-specific system.

## 1.4 Intended audience

This document has the objective to communicate with EU institutions and stakeholders interested in system security and relevant certifications when applicable.

## 1.5 Out of the scope

The editorial team of this document intentionally decided to not address supply chain needs for systems with the intention to cover this extensive topic in another dedicated ECSO document. The data privacy aspect related to GDPR is not treated in this document.

Specific recommendations for securing a system will be addressed in a dedicated ECSO document.

This document will not focus on the security of an OT or IT system, but instead puts efforts on their commonalities.

# 2 System security description

This section intends to describe initial concepts and definitions that help better characterise what systems are, their cyber security need and how they differ from a product security perspective. Those concepts may vary according to the system's size, functional diversity, complexity, and implementation constraints.

## 2.1 System definition

A simple acceptable definition of a system, derived from the NASA system handbook [1] would be:

A "system" is the combination of elements that collaborate to produce the capability required to meet a need.

The elements consider all assets including hardware, software, services, data, equipment, communication networks, facilities, personnel, processes, and procedures needed for this purpose; that is, all things required to produce system-level objectives. The objectives include system-level qualities, properties, characteristics, functions, behaviour, and performance.

The value added by the system as a whole, beyond that contributed independently by the parts, is primarily created by the relationship among the parts; that is, how they fit together and are orchestrated.

**The system's mission in this document is to be understood as a system instantiation and customisation to a precise use case and context.**

## 2.2 Difference between system security and product security

For a good comprehension of the following sections, it is important to highlight that systems and products have different perspectives of what is needed in terms of security.

It is normally accepted that product security can derive from the knowledge of the intended use of a product, its risk assessment and associated mitigation controls.

Systems rely on different manufacturers and products combined in ways that create large quantities of new system-specific use cases, dealing with constraints such as safety, real time performance, data privacy and lifespan that could last 20 years or more.

When dealing with system security, most of the challenges and complexities lay on the evolving system level features during its lifespan, associated risk management, evolving architectures, business objectives and the management of a multi stakeholder system engineering process.

Systems will have customised security measures adopted following the risk assessment, and the system owner will have an active role on the implementation and maintenance of those measures all along the system's lifecycle.

## 2.3 EU regulation security requirements

The European Commission has recently published its cyber security strategy for the digital decade, with a proposal for a directive on measures for a high common level of cyber security across the Union, replacing the 2016 NIS Directive and launching a new critical entities resilience directive (2020/0365 COD) [2] replacing the 2008 directive on European critical infrastructures.

This strategy has the goal to improve Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy, reliable services and digital tools.

Among the many actions adopted by the European Commission, the one that impacts the most digital systems is the NIS2 Directive [3], which puts under its reach two new groups of EU actors now named *essential entities* and *important entities*.

The Directive puts in place several requirements from governance to cyber security risk management, reporting, supervision, and enforcement. All articles are part of the mission specific requirements and should be considered as legal objectives of the systems to be deployed in the EU and, in this document, case special attention should be observed in article 18 and article 21, covering cyber security risk management measures and the use of European cyber security certification schemes (Regulation (EU) 2019/881 [4]).

# 3 System security concerns

Systems are built for many complex use-cases, with large diversity of products, functions, quantity of suppliers, internal and external processes, and professional workforce. Systems security is a very challenging exercise to system owners, which is described in the following chapters.

Examples of system type can be found in Annex 2.

## 3.1 Security governance

Building resilience is the way to incorporate the ability to identify and adapt to risk by aligning organisational and technical capabilities to achieve an effective and efficient operational risk management. It is still a common belief that business continuity is just a technology problem that must be solved by the technical personnel within the organisation, by applying redundancy and proper backup and recovery planning to the information or operational system. However, legal, financial, communications, human resources and organisational training are all aspects that have to be considered when building operational resilience for an organisation. Security policies, processes and procedures coordinate the operational activities performed by people and technologies with a specific organisational mission.

Supply chain security is part of the system security governance. As explained in Section 1.5, this extensive topic will be covered in another dedicated ECSO document.

The security resilience of these organisations is dependent on the proper security management, identification, and security risk assessment of the critical assets, as well as on the implementation of adequate security risk mitigating measures. The objective is to keep the focus on the business mission, delimited by a defined and known risk appetite and tolerance.

Organisations must ensure that the necessary procedural and technical controls are implemented and enforced to protect the designed, implemented, and operated systems from their requirements and specifications phase until their end of life. The usage of international standards, frameworks and recommendations that are referred in the ECSO SOTA document [5] is strongly recommended.

As an example from an industrial environment (cf. Annex 2), the ISA/IEC 62443 [6] international framework for security in industrial automation and control systems defines requirements for security in organisations, technology, and people in all phases of the system's lifecycle, from product development, through system integration and through the entire operational phase. In combination with the ISO 27001 [7, 8] international standard (ISA/IEC 62443-2-1), which defines establishing, maintaining and continuous improvement of security controls for an Information Security Management System (ISMS), this would build a strong foundation for security governance in the organisation.

## 3.2 System security lifecycle and threat landscape evolution

The system is mission-specific and will be assembled to cope with needs and requirements defined by the system's owner. In addition, the functional perimeter of the system (new functions, business adaptation, etc.) could evolve over time. Systems will normally last longer than many of the products they are built on, and their threat landscape will probably evolve significantly during their operational life.

Therefore, it is expected that system owners will deal with constant technical evolutions, different versions of components, cyber security maturity and maintenance tasks that increase in complexity during time.

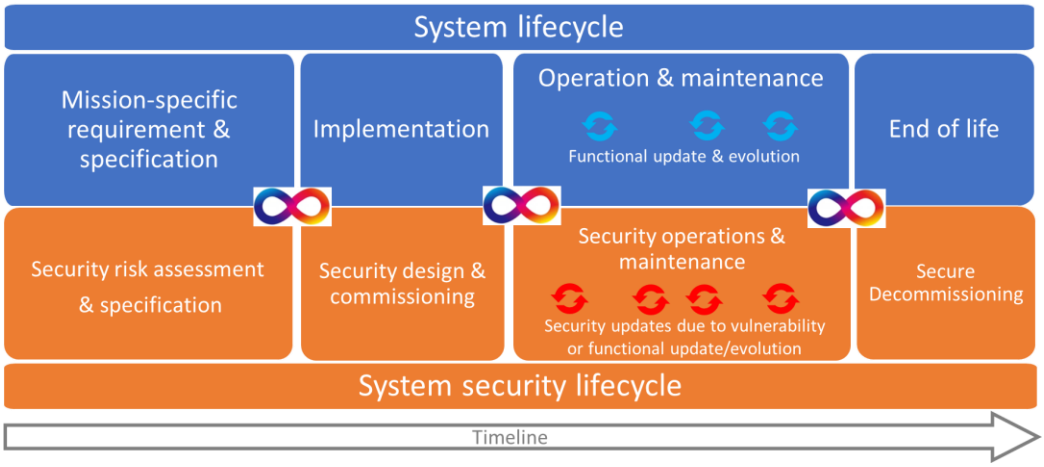



**Figure 1** - Intertwined functional and security lifecycle

Functional and security requirements must be treated in a permanent interaction and in an agile mode, adding new security controls when needed to maintain security posture over time (all along of the lifespan of the system) either due to the threat landscape evolution and/or to the permanent functional evolution of the IT or OT system (Figure 1).

Starting from the identification of assets involved in the system, it is important to notice that the periodic security risk assessment to be performed should consider risks of different nature and vectors such as:

- all operational processes,
- system contexts (IT, OT, on premise, cloud, etc.) and constraints (safety, etc.),
- product particularities (age, embedded technology, etc.),
- data and its criticality,
- automatic or human-initiated interactions to all functions performed at system and product level.

The identified system risk must be correctly addressed and kept at acceptable levels.

It is also important to notice that system security will require recurrent and/or specific security activities in the different lifecycle phases, such as:

- awareness & training,
- security risk assessment,
- secure architecture,
- security test & validation,
- vulnerability management (updates, patches, etc.),
- information sharing,
- security process management, not only at asset level but also at system level.

As an illustration, let us consider the water treatment system example described in Annex 2. The key objective is to ensure the respect of sanitary measures, confidentiality, and integrity of the industrial process, as well as ensuring security of products or any other physical instrumentations.

## 3.3 System stakeholders: roles and responsibilities

Various stakeholders with different objectives are involved in the system lifecycle (specification, implementation, operation, maintenance, and decommissioning), which implies many interactions among them. Those stakeholders include, for instance, the system owner, system operation/maintenance personnel, system installation/integration personnel, product suppliers/vendors and potential end users.

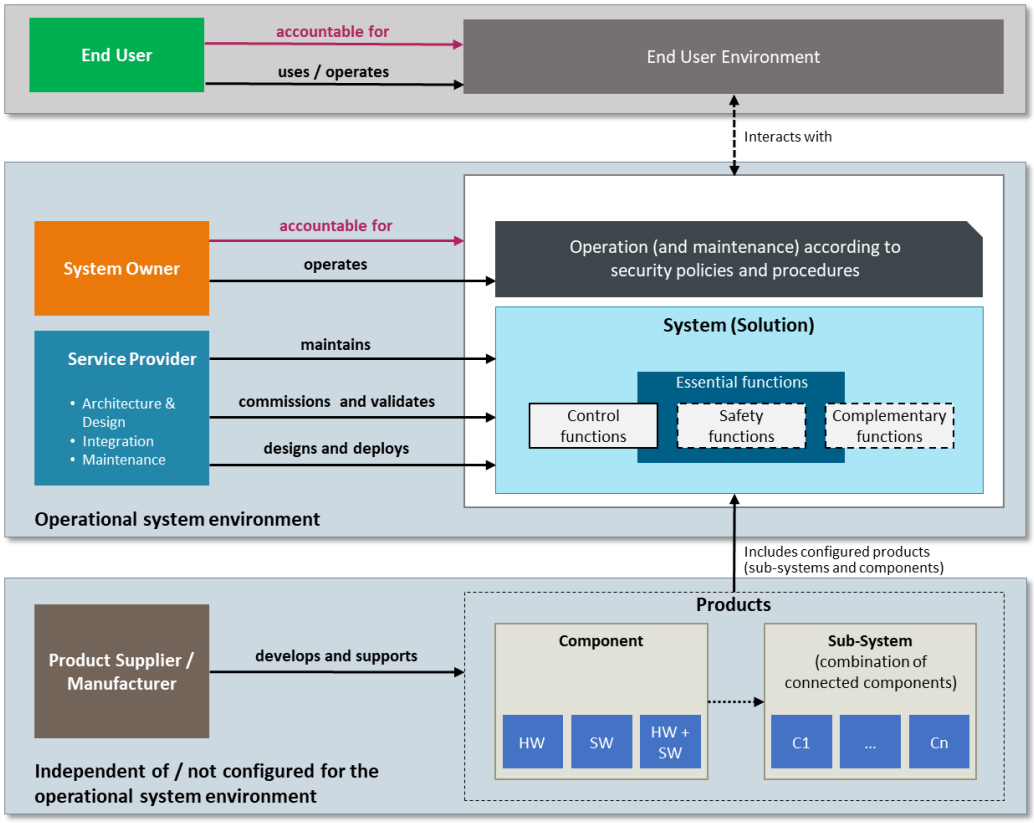



**Figure 2** - System stakeholders

Figure 2 addresses the four major roles involved during the system lifecycle: end user, system owner, service provider and product supplier/manufacturer. Each role includes a specification of the assigned activities and responsibilities. A role needs to be assigned to an entity that takes ownership for the corresponding activities and responsibilities. Multiple roles can be assigned to a single entity, for instance, the system integrator might accomplish the integration and the maintenance tasks of the system.

**Table 1** – Stakeholders' role

| Role | Description |
|---|---|
| End User | User of the data and service provided by the system in respect to the cyber security policy.<br><br>*(End user is optional, as not every system allows the end user interaction)* |
| System Owner | The System Owner (SO) includes two roles. The first role is the accountability for the system security (legal) and the second role is to operate the system according to defined security policies and procedures. |
| Service Provider: Design and integration | The integration Service Provider (SI) is responsible for the design implementation, commissioning, testing and validation of the security measures applied to the system (mission-specific). |
| Service Provider: maintenance | The maintenance Service Provider (SM) is responsible for the security maintenance and decommissioning of the system. |
| Product Supplier / Manufacturer | The Product Supplier (PS) is responsible for the development and support of products, including the security aspects, used in the system (mission-specific). |

As described in Table 1, many professionals working for different stakeholders could perform all sorts of activities during the system lifecycle, with different specialisations and with different objectives in mind.

Considering this workforce as any workforce, this shall be composed of professionals with different experience levels and backgrounds. It becomes imperative that they can be managed uniformly by the organisation they belong to and share the same security risk comprehension.

## 3.4 Domain expertise

Each business domain (e.g., automotive, healthcare, cloud, financial, etc.) needs a huge expertise to address its functional constraints and specificities, such as:

- business objectives,
- system intended use and operational environment,
- Service Level Agreement (SLA),
- regulatory requirements.

Traditionally, safety and security have been considered separately, but due to the growing recognition of the mutual impacts, a combined view becomes more important. The key point is that cybersecurity, privacy, and physical safety can no longer be treated as separate concerns.

System security stakeholders must know and consider these constraints in order to build a specific cyber security expertise. They must manage cyber security recommendations, relevant and adapted to the domain. A continuous update and actualisation of the cyber security expertise is needed to cope with the evolution of a system and domain.

## 3.5 Responsibility and cyber risk transfer between stakeholders

The design, implementation, operation, and maintenance of the security of the system implicates numerous stakeholders for the different security tasks in each lifecycle phase.

The stakeholders and the system owner are confronted with the challenge of:

- being able to protect the system and maintain security during its different phases,
- ensuring clear understanding of the cyber risks and their impacts on stakeholders,
- establishing and addressing limits of responsibility among stakeholders and during transition phases,
- ensuring traceability throughout all stages of the supply chain.

This implies a formal transfer of responsibility and associated cyber security risks among them.

## 3.6 Security architecture and design challenge

A system brings many complexes uses cases, diversity of products, manufacturers and functions. The conceptualisation of a secure architecture and design is a challenging task, in which a right balance between the mandatory evolution due to business development (new processes, new products on the market, acceptable risk for the business organisation, insurance discounts, tax incentives or legal obligations), the diverse system constraints (e.g. product life span, operational environment, mixing legacy and new products, the evolution of the technologies, etc.) and the constant evolution of cyber security attacks, both internal and external, should be considered.

Applying best security practices, principles and engineering process is key to addressing these challenges at architecture level.

## 3.7 Vulnerability and incident management challenge

When the system is in operation, it will be exposed to incidents or several types of vulnerabilities at different component levels.

A system security check and exchange with product suppliers or relevant CERT (Computer Emergency Response Team) will help the system owner to be informed about vulnerabilities. As an example, the ISO/IEC 30111 [9] standard could be considered.

When a vulnerability is identified, the system owner is confronted with the challenge of:

- assessing the exploitability,
- assessing the impact for the system and business operation,
- identifying the possible mitigations (compensation countermeasures, configuration change, product patching, organisation change, etc.),
- finding the solution that will be a trade-off based on the business risk appetite (legal, economical, etc.) and operational limitations,
- timely response from product vulnerability discovery,
- information sharing asymmetry among stakeholders.

With the available information, the system owner will take the decision regarding his/her best choice considering the business continuity and cost impact to mitigate the risk.

In case of an incident, a CERT is also necessary to handle the incident response lifecycle (planning, prevention, detection, containment, remediation, recovery & restoration, and post incident analysis).

For incident management, in the context of previously described system complexity and permanent evolution, the system owner is confronted with the following non-exhaustive list of challenges:

- have an updated list of critical assets,
- be able to set and update continuity plan document,
- be able to conduct relevant operational exercises following the defined continuity plan,
- be able to obtain a clear context of the incident, assess the impact for the system and business operation and consequently set action priorities,
- to obtain a timely response compatible to the business process criticality.

Those challenges must be addressed in anticipation by the system owner in order to limit damages.

## 3.8 Cyber security interoperability

Systems evolve rapidly inside organisations, being a natural reflex of business development, evolving processes, new products on the market or legal obligations. This characteristic, added to a diverse product life span and a large variety of models and manufacturers, drives system owners to face strong challenges of cyber security interoperability requirements for their systems, for the

needed evolutions, replacements, retrofits and even decommissioning in a coherent security framework.

To provide interoperability for the information exchange between assets, a system must include communication interfaces, information security and data model specifications. The objective of interoperability in this context is to ensure that system owners can select, assess/evaluate, and approve different market players capable to provide services, products and solutions that rely on a common security implementation understanding.

# 4 Certification considerations

In the previous chapters, it has been underlined that a system is assembled and run according to the objectives of its lifecycle phases and will be put in permanent evolution and constant improvement for business efficiency to deal with an evolving threat landscape.

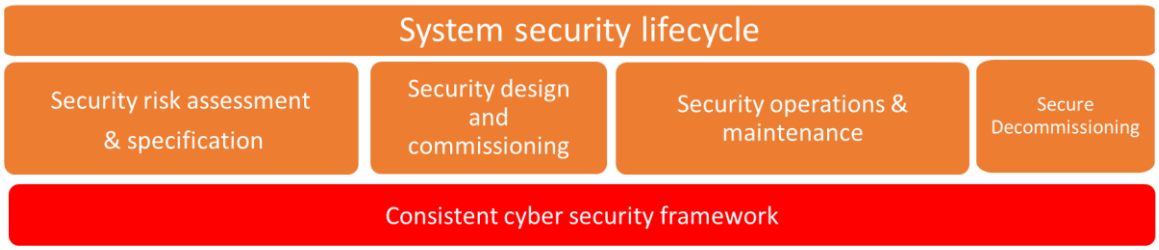



**Figure 3** – Comprehensive cyber security framework

Different security frameworks could be considered as reference for system security, all depending on the type and nature of the targeted system. The most common ones are NIST framework [8], ISO/IEC 27000 [10] and ISA/IEC 62443 [6]. It must be highlighted that these frameworks are not mutually exclusive and can be applied together in coordination or independently, depending on the targeted system.

The importance of an efficient security governance, security risk management process and secure engineering become clear aspects. These key processes will contribute to reaching a higher organisation security maturity level.

In this context, a single certification encompassing the whole system's needs is not only irrelevant, but also technically and economically unrealistic. Nevertheless, different relevant certifications with dedicated objectives will help the system owner reach the overall system-targeted security level objectives.

At the initial lifecycle phases, before the deployment of the system, the pertinent certifications are more related to products, processes, and services, such as systems design, engineering and architectures, system integration and validation processes, product security capacity and supply chain (provisioning and procurement).

**Table 2** – Examples of certifications related to the initial lifecycle phase of a system

| | Example of related certifications |
|---|---|
| **High level & detailed Risk assessment** | ISO/IEC 27005 [11] risk manager certification (people). |
| **Architecture & design** | IECEE ISA/IEC 62443-3-3 [12] network and system certification (reference architecture). |
| **Supply chain** | Example of product certification: CSA compatible certification (EUCC), NLF conformance, CSPN, BSZ, LINCE. |

| | |
|---|---|
| **Process, development process** | IECEE ISA/IEC 62443-4-1 [13] Secure development lifecycle,<br>ISO/IEC 27034 [14] application security lead implementer & lead auditor. |

Once the system is deployed at production stage, the pertinent certifications are more related to process and services with focus on secure operations, patch management, vulnerability, and management.

**Table 3 –** Examples of certifications related to the production lifecycle phase of a system

| Example of related certifications | |
|---|---|
| **Secure integration & commissioning** | IECEE ISA/IEC 62443-2-4 [15] IACS service providers,<br>GIAC Global Industrial Cyber Security Professional (GICSP). |
| **SecOps** | ISACA Certified Information Systems Auditor (CISA).<br>GIAC Certified Incident Handler, GIAC Response and Industrial Defense (GRID).<br>ANSSI IT Security Auditor (PASSI = Prestataires d'Audit de la Sécurité des Systèmes d'Information qualifiés France). |

During the system's lifecycle at governance level:

**Table 4 –**Examples of certifications related to the governance / process level of a system

| Governance / process level related certifications | |
|---|---|
| **Organisation with a well-defined mission** | ISO/IEC 27001 [7] Information security management system.<br>ISO/IEC 27001 [7] Lead implementer & lead auditor.<br>ISA/IEC 62443 [6] (OT) Cyber Security Management System. |

Nevertheless, with this collection of possible certifications there is a need for coordination, management and monitoring in real life systems, and such action can become a true challenge to systems owners. One example of such challenge can refer to system owners that are managing systems of systems.

System owners may have a large quantity of individual product certificates. They can differ in assurance levels and validity, causing additional challenges and raising questions on the real need of individual certificates after procurement.

What is currently understood and shared among system owners is that the importance of the individual product certificates decreases in time once procurement stage is passed. While performing regular system risk assessments, new security measures are put in place to deal with evolving security challenges, and individual product certificates become less relevant than a collaboration for vulnerability management with system suppliers.

# 5 Conclusion

As discussed in the previous chapters, system security is not the sum of individual product security certificates, but rather a security lifecycle complex journey engaged by system owners. This journey must be driven by a strict governance with security processes in mind, targeting highly customisable business objectives. In a world under constant digital transformations, systems have their functional characteristics and perimeters put in constant evolution, therefore facing an increased attack surface on top of an evolving threat landscape.

System security challenges will continue to increase and diversify following systems specialisations in the different domains of application. It is important to observe that system security priorities change according to system objectives and types, which is why technical expertise in the targeted domain is a real success factor in system security. As an example, an OT system with specific constraints for process safety may require specialised security controls.

In this context, a single system certification might not be a realistic objective for systems. A solution to maintain the security posture overtime is to support the certification and continuous assessment of the processes and qualified personnel.

ECSO Members see positively all efforts from the European Commission to create and act directives aiming to deal with those challenges such as the NIS2 [3] revision or the work done with ENISA under the CSA (Regulation (EU) 2019/881 [4] [14]) to make a toolbox of possible specialised and complementary certifications available to stakeholders.

Those constraints and tools will help system owners reach a higher level of security and organisation maturity in their daily system operations. To speed up and boost the security of a system, it is important to give the right priority under the Union Rolling Work Programme (URWP) to service and process activities due to their critical contribution to systems security.

# 6 Bibliography


[1] NASA, “NASA Systems Engineering Handbook,” 2007.

[2] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the resilience of critical entities. COM(2020) 829 final,” December 2020.

[3] European Commission, “Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. COM(2020) 823 final,” December 2020.

[4] European Parliament, Council of the European Union, *Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

[5] European Cyber Security Organisation (ECSO) WG1, *State-of-the-Art Syllabus: Overview of existing Cybersecurity standards and certification schemes v2.0,* Brussels, December 2017.

[6] ISA/IEC 62443, “Security for industrial automation and control systems”.

[7] ISO/IEC 27001, “Information technology -- Security techniques -- Information security management systems -- Requirements,” 2013.

[8] NIST, “Framework for Improving Critical Infrastructure Cybersecurity v1.1,” April 2018.

[9] ISO/IEC 30111, “Vulnerability handling processes,” 2019.

[10] ISO/IEC 27000, “Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary,” 2016.

[11] ISO/IEC 27005, “Information security risk management,” 2018.

[12] IEC, “IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels,” IEC, 2013.

[13] ISA/IEC 62443-4-1, “Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements,” 2018.

[14] ISO/IEC 27034, “Application security managment process,” 2018.

[15] ISA/IEC 62443-2-4, “Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers,” 2015.

[16] NIST, “SP 800-160 Systems Security Engineering,” 2018.

[17] ISO/IEC 2382, “Information technology — Vocabulary,” 2015.

[18] ISO/IEC TR 23188, “Information technology — Cloud computing — Edge computing landscape,” 2020.

[19] ISO 31000, “Risk management — Guidelines,” 2018.

[20] NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” 2013.

[21] ISO/TR 25102, “Intelligent transport systems — System architecture — 'Use Case' pro-forma template,” 2008.

# Annex 1 Glossary

The definitions reported hereafter integrate those taken from ECSO's glossary. Some terms have been refined in accordance to the Cybersecurity Act [4] and to the current context. In such case, all applicable definitions are reported.

| Term | Definition / Explanation |
|---|---|
| Asset | An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Source: NIST SP 800-160 [16]. |
| Assurance level | "'Assurance level' means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned". Source: Cybersecurity security Act [4]. |
| CERT | Computer Emergency Response Team. |
| Certification | Formal attestation or confirmation of certain security properties of an organisation, system, component, or product. |
| Component | One of the parts that make up a product or a system. A component may be hardware or software and may be subdivided into other components. |
| End-User | Person or organisation that ultimately uses or is intended to ultimately use a system or a product. |
| Feature | An aspect of functionality that in combination with other features serves to enable but not define the purpose of the product component or system. Features have many use cases. |
| Functional feature | An aspect of functionality that in combination with other features serves to define the purpose of the product component or system. Features have many use cases. |
| IT System | Processes Information processing system, together with associated resources such as human, technical, and financial, that provides and distributes information ISO/IEC 2382 [17]. |
| OT system | Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices and systems, processes, and events within the organisation. |

| Term | Definition / Explanation |
|---|---|
| | ISO/IEC TR 23188 [18], 3.2.7. |
| Process | Set of interrelated or interacting activities which transforms inputs into outputs. |
| Product | It includes goods (device, software, hardware, etc. ready to be used, but also products that are designed to be easily installed and to interoperate with existing system components). |
| Product Supplier | The role Product Supplier (PS) is responsible for the development and support of products used in the system (mission-specific). The activities include the development of product security capabilities to be used in the system following an established product development life cyclelifecycle process, including incident handling and vulnerability management processes. The PS has the responsibility for the provision of product-specific integration and hardening and setting operational guidelines for the product(s) he/she supplies to the System Owner (SO).<br>• *Develops, maintains, and supports products (components or sub-systems) throughout the product lifecycle.* |
| Requirement | Need or expectation that is stated, generally implied or obligatory. |
| Residual risk | Risk remaining after risk treatment:<br>Note 1 to entry: Residual risk can contain unidentified risk.<br>Note 2 to entry: Residual risk can also be referred to as “retained risk”. |
| Risk | Effect of uncertainty on objectives. Reference to ISO 31000 [19] and ISO 27001 [7]. |
| Security Capabilities | A combination of mutually reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals). NIST SP 800-53 [20]. |
| Security Objectives | Goals and constraints that affect the confidentiality, integrity, availability, authenticity and traceability of your data and application. |
| Security reference architecture | A cyber security reference architecture consists of a set of documents that contains cyber security best practices and recommendations on the structure and integration of the products, services, and functions necessary to build a system. It guides the secure implementation of complex technological solutions. |
| Service provider: design & Integration | The role integration service provider (SI) is responsible for the design and implementation, as well as commissioning and |

| Term | Definition / Explanation |
|---|---|
| | validation, of the security measures applied to the system (mission-specific). The activities cover the development and validation of a robustness and resilience program for the system in operation with the goal to match the tolerable cyber security risk. These include the development of technical security measures applied to the system, as well as guidelines for organisational measures to be implemented during an operation. The base for the guidelines is often given by guidelines provided by the role product supplier. It is not unusual that one or several organisations design and deploy parts or the whole system while another organisation is responsible for commissioning and validating the system.<br>• *Defines the system security architecture according to the risk analysis and the associated requirements.*<br>• *Designs, integrates, and deploys the system according to the requirements defined by the system owner.*<br>Integrates products to the system according to the specification. |
| Service provider: Maintenance | The role maintenance service provider (SM) is responsible for the maintenance and decommissioning of the system. Compared to the actualisation of the information used in the security measures, which is included in the role SO, the maintenance activities have the purpose to upgrade and eventually complement the measures of the robustness and resilience program to follow a change in the threat situation, a change on business risk approach by the SO or a modification of the system. A maintenance phase is triggered by the result of a cyber security risk assessment showing that the measures of robustness and resilience program no longer provide the desired level of protection. In general, the upgrade includes technical security measures applied to the system, as well as the organisational security measures for operation of the deployed Defence-in-Depth model to keep the desired protection of the system in operation. The SM includes the responsibility for decommissioning either parts or the whole system and ensuring that the tolerable residual cyber security risk is still matched during or after decommissioning.<br>• *Maintains a system according to the requirements defined by the system owner.* |
| Specified requirements | Need or expectation that is stated. Specified requirements may be stated in normative documents, such as regulations, standards, and technical specifications. |
| Sub-system | One or more elements of a system that meet the same functional need, the same security criteria (same level of security of data and |

| Term | Definition / Explanation |
|---|---|
| | processing, availability, integrity, and confidentiality) and which have the same level of exposure (accessible to users, isolated system, etc.) |
| System Owner | The System Owner (SO) includes two roles. The first role is the accountability for the system (mission-specific), including the protection of the system in operation and the associated risks throughout the life cyclelifecycle.<br>The SO defines the tolerable cybersecuritycyber security risk as an input requirement for all cybersecuritycyber security activities along the system life cyclelifecycle. Whilst remaining accountable, the organisation fulfilling this role delegates the responsibilities and the associated activities to organisations fulfilling other roles described in this clause.<br>The role assigned to the SO refers to the responsibility to operate the system according to defined security policies and procedures. It includes keeping information used in security measures, such as virus patterns, firewall rules, active accounts list, or backup and restore data up to date. The inclusion of these two roles covered by the SO considers that in many cases the organisation which operates the system is also the legal owner, and therefore accountable for the system. |
| Threat | Potential cause of an unwanted incident, which can result in harm to a system or organisation. |
| Use Case | “Use Cases” are a means to define requirements for a system in terms of the primary users (known as actors) that interact with the system and the scenarios or activities that are performed by the system in response to stimuli from the actors or from other system entities. Each “Use Case” has a starting state and conditions, a series of activity steps that together comprise a scenario, and a finishing state and conditions. There may be more than one scenario in a “Use Case”. The “Use Case” should also include exceptional cases with alternate outcomes. (ISO/TR 25102) [21]. |
| Vulnerability | Weakness of an asset or control that can be exploited by one or more threats. |

# Annex 2 Examples

**Industrial Control Systems: Water and Wastewater Treatment**

Water is called the elixir of life as it provides essential minerals to humans. Although more than 70% of earth is covered in water, providing potable water is becoming more challenging. Water and wastewater treatment facilities are an essential need for any town or a city. The drinking water is treated properly to remove the dissolved solids, pollutants, and pesticides to ensure it is safe for drinking.

Water treatment is an industrial process. A water treatment facility will have three networks:

- *pumping network,*
- *water treatment,*
- *water distribution network.*

The pumping network will have huge pipelines and pumps which will pump natural water from water sources like rivers, ponds, and lakes. The pipelines might run several kilometres and have water pumps in multiple stages in distributed locations. Water is filtered and treated using a chemical process in the water treatment facility and stored in overhead tanks. The distribution pipeline delivers the drinking water to homes. Metering the water consumption, detection of leaks and service outage due to pipe damage are monitored in the distribution network.

Existing water treatment facilities have generally been in operation for more than 50 years, requiring a continuous update of the plant to meet customer requirements and to drive operational efficiency. This water treatment facility requires many different systems like Industrial Automation and Control systems (IACS), electrical distribution system, building management system and more. Therefore, several Industrial Automation and Control systems (IACS) are required to automate, remotely control, and monitor assets (pumping, storage, processing, and distribution), needed to manage the geographically dispersed operations of a water treatment facility. This system must ensure the basic process control, but also the safety aspect.

Thereby, there are several aspects to cover for the security point of view of system:

- *Physical security (fences, pipeline monitoring solutions, leakage detection systems, facility monitoring solutions, etc.)*
- *IT (ERP servers, billing, and payment application, etc.)*
- *Network (IT & OT)*
- *OT Industrial Control System (Scada, PLC, sensor/actuators and instrumentation)*

Many concerns at the system level:

- *Big number of devices with different versions /models, etc, process assets (Mechanical device, etc.)*
- *Legacy device and software*
- *Interconnection of system and devices depends on system design*
- *Large number of stakeholders (employee, contractor; supplier, etc.)*

Several Requirements and constraints to consider:

- *Safety (risk of water contamination …) & environmental (pollution) regulation*
- *High availability 24/7*
- *Lifespan of the industrial system*
- *Continuous maintenance phase (update, recycle, retrofit, revamping).*

**A maritime HR system as an example of a smaller system.**

A Maritime HR system at a high level of cyber security requirement must address various concerns not uncommon with HR systems in other verticals with a few additional concerns.

Examples:

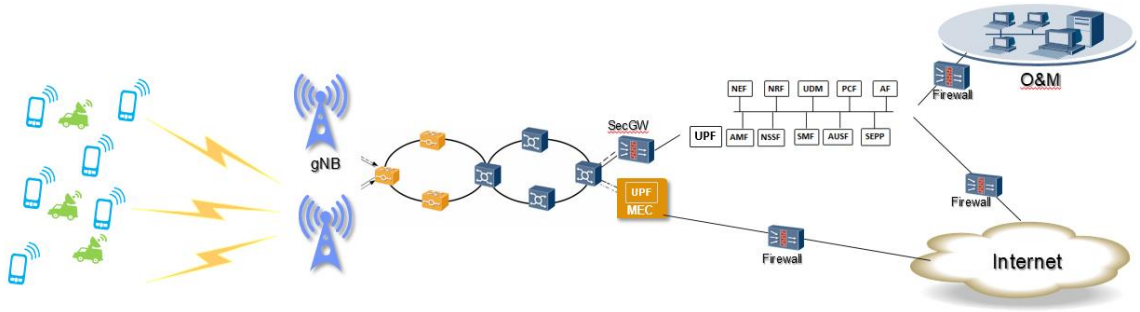
- *The protection of personal data from an extraction forms a secure environment. Secure storage ad extraction of sensitive information.*
- *The protection of personal medical records forms unauthorised access even internally in the marine enterprise.*
- *To protect against the effect of cyber security breaches and unauthorised changes to information. Especially information sent to third parties such as port security and immigration departments that depend on the veracity of such information.*
- *The protection of payroll aspects of the systems from diversion of funds forms the intended party.*
- *Corroboration, to ensure or warn that authorised access has not been compromised by means, for example of impersonation of internal authorised actors.*

The above aspects require that every path of propagation of use cases that affects the above cyber security requirements is adequately secure commensurate to the analysis and establishment of the risk.

This is turn involves the following examples, which introduce complexity by a sheer number of use cases and related propagation paths:

- *Secure design, anticipation of the propagation paths of illicit intrusion that result in risk, and mitigating measures designed into the system.*
- *Security in the deployment of the system with adequate deployment and end user expertise.*
- *Security of subsystems such as power supply, subordinate systems, and components, underlying operating systems, underlying sub-systems provided by external manufacturers.*
- *The changes made to these subsystems by external manufactures and their effect on cyber security have been anticipated.*
- *The improvement to the system features, as demanded by system revisions and as requested by clients, as well as the changes made to non-functional and sub systems are tested for cyber security vulnerabilities,*
- *Tests on sufficient use cases of the revisions are run to ensure that combinations of use cases are secure.*
- *Secure means of updating of the system that minimise potential illicit interventions.*
- *Means to help the stakeholders and the end users to familiarise with the upgrades made to the system.*
- *The need to adjust certification to the complexity of the above.*

**5G Ecosystem:**




A 5G Network infrastructure is made of several components such as:

- *IoT devices.*
- *Radio access network equipment for the end2end communication.*
- *An operation & maintenance platform.*
- *Core network components (e.g., multi access edge computing platform;)*
- *Cloud platform & services.*
- *Network equipment and applications (router, gateway, switch, etc.).*
- *Applications.*

Challenges for the E2E certification:

- *Complexity & heterogeneity of the components.*
- *Number of stakeholders (equipment provider and its supply chain, network operator (admin, end user), etc.)*

ECS
EUROPEAN CYBER SECURITY ORGANISATION

## > JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU