TNO innovation for life

Cyber resilient system design methodology

TNO Public ⟩ TNO 2025 R10875
30 April 2025

ICT, Strategy & Policy
www.tno.nl
+31 88 866 50 00
info@tno.nl

TNO 2025 R10875 – 30 April 2025

Cyber resilient system design methodology

Author(s)	Acur, Sezen; Das, Swarna; Leeuw, Bas van der; Vasenev, Alexandr; Goosen, Pieter (PM)
Classification report	TNO Public
Title	TNO Public
Report text	TNO Public
Number of pages	46 (excl. front and back cover)
Number of appendices	0
Sponsor	ISP
Programme name	ERP Cyber-secure systems by Design
Project name	Cyber resilient system design

This work is intended for an audience with a foundational understanding of cybersecurity and systems engineering. The methodology and concepts discussed are framed to be accessible to readers who possess prior knowledge in these fields and are familiar with the context and background of the problem space addressed in this work.

Contents

List of Figures

1 Introduction

As digital systems become increasingly integral to society, cybersecurity has become a fundamental requirement due to rising cyber threats and incidents. At the same time, the systems requiring protection are growing more complex and exposed, making reactive approaches insufficient.

There is a pressing need for inherently cyber resilient systems, those capable of preventing, withstanding, and recovering from cyber incidents to ensure mission continuity, reduce damages, and lower life-cycle costs [1]. In addition, the standards related to cyber-resilience and systems engineering are not applied, tailored, and/or introduced according to the needs of the businesses.

A lack of resilience can lead to component failures with potentially widespread economic consequences. For example, a cyberattack on semiconductor equipment could disrupt the chip-making industry, while other incidents such as compromised document printing, hospital ransomware attacks, or airport luggage system failures can cause significant personal and organisational disruption.

TNO is addressing these aforementioned challenges through a multi-disciplinary Exploratory Research Programme (ERP), in which research line 1 (RL1) focuses on developing a methodology for cyber resilient system design. The approach described herein, integrates cybersecurity and resilience into systems engineering, based on input from specialists in security, safety, and systems engineering, all of whom affirmed the methodology's relevance to their roles.

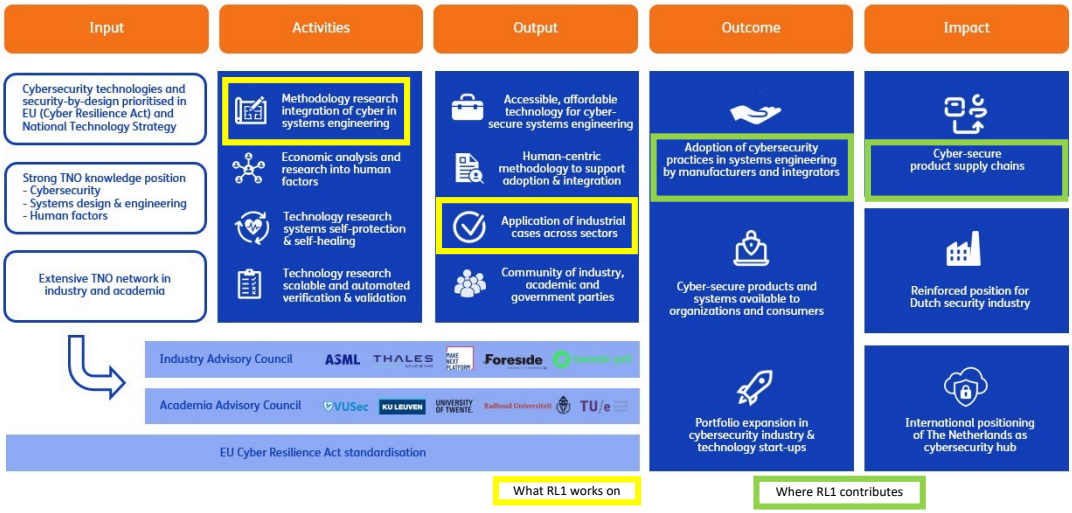

Figure 1: The impact pathway of the ERP Cyber-Secure Systems by Design and where RL1 contributes [2].

2 The Methodology Overview

Systems Engineering (SE) [3] is an interdisciplinary field focused on developing systems that fulfil specific purposes or needs. Across its life cycle, SE involves design, integration, validation, verification, and future system management. As systems become increasingly complex and interconnected, SE must account for broader ecosystems to manage these complexities.

In the traditional systems engineering process, safety and security are ‘bolted on’ after the system architecture and decomposition are determined and delegated to specialty engineering disciplines [4]. ‘Bolted-on’ safety and security as specialty engineering after the system design is not effective anymore. This sentiment is echoed in the INCOSE Vision 2035, [5], in which Systems Engineering is expected to incorporate safety and security in the SE development life cycle.

Motivated by this vision, a cyber resilient systems methodology has been developed. This methodology integrates cyber resilience and security from the early conceptual phase of the system life cycle (shown in blue star), using an iterative and recursive approach supported by clearly defined roles.

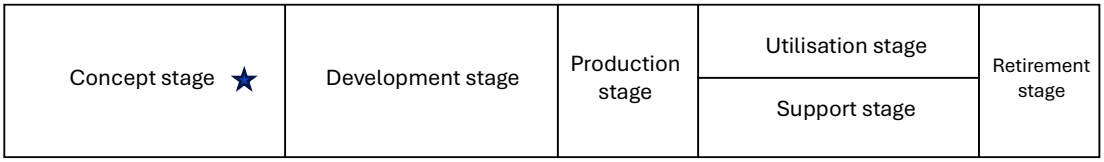

Figure 2: The ISO 15288 Generic Life Cycle.

The methodology operates across four levels:

- **Level 0:** Explains the methodology in the context of a System of Systems (SoS).
- **Level 1:** Provides a meta level overview including involved roles.
- **Level 2:** Outlines a step-based workflow.
- **Level 3:** Focuses on the execution of tools and methods, referencing applicable standards and frameworks.

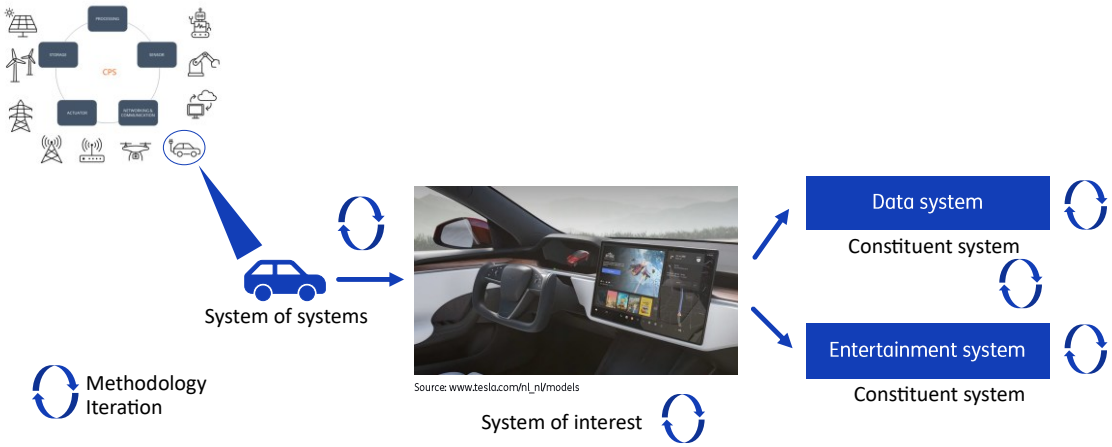

Figure 3: Level 0 demonstration of the methodology.

To illustrate this, a cyber-physical system is examined. A system of interest (e.g., a vehicle's display system) is selected from the SoS, and the methodology is applied to its constituent systems (e.g., data and entertainment systems). The process is iterated to ensure both the systems and their interfaces achieve cyber resilience, and then scaled back up to the system of interest and the full SoS. This is where level 1 and level 2 processes are applied.

Level 3 involves applying standards and frameworks, which may vary across different domains. Future industry use cases and security-related projects will help refine how these are implemented. Several level 3 examples are included in Appendix A.

In the following sections outlining the step-based workflow, some figures include directional arrows while others do not. This variation reflects the fact that certain workflows adhere to established standards and regulations, whereas others may differ depending on customer requirements or changes in the domain. Although the methodology presented is domain-agnostic, we anticipate that adaptations will be necessary when applied to real-world industry scenarios where domain-specific considerations come into play.

Part of the methodology is inspired by the Cyber Security Requirements Methodology (CSRM) from SERC [6] and in compliance with parts of IEC 62443 [7]; ISO 15288:2023 [8], ISO 829 [9]; NIST 800-160 V2 [10], NIST 800-37 [11], and NIST 800-12 [12].

2.1 The Meta level methodology

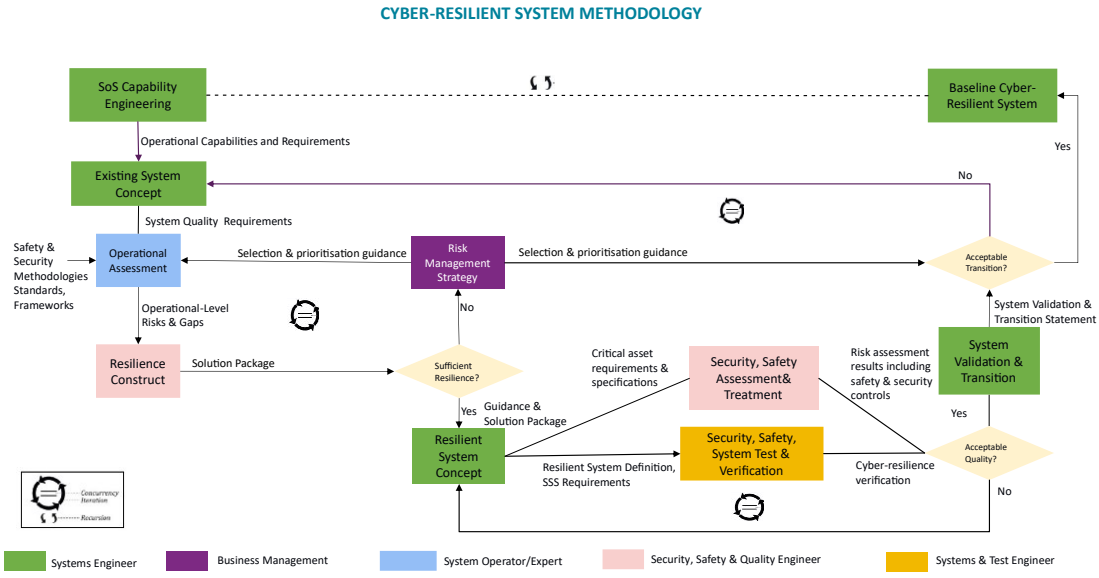

Figure 4: Meta level methodology

The meta level methodology begins with the systems engineer conducting SoS capability engineering. In this phase, the operational capabilities and requirements of the SoS are identified, ensuring that constituent systems play defined roles in achieving these capabilities within the system of interest. The existing system concept refers to one of these constituent systems for example, the data system or entertainment system, as illustrated in the level 0 example. Importantly, the methodology can be applied to multiple constituent systems simultaneously; there is no need to follow a sequential order. These systems are treated as brownfield cases as they are operational and functional from a systems engineering perspective, but not yet cyber resilient. Once cyber resilience is achieved, the system is regarded as a greenfield case.

From the existing system concept, system quality requirements are extracted. These include cyber resilience, security, and safety. An operational assessment is then carried out by the system operator or a domain expert to identify potential vulnerabilities and issues in the system's operation. Various safety and security methodologies and frameworks may be applied during this phase, executed at level 3.

The business manager addresses risk on multiple levels, focusing on safety, security, and overall system risk. In systems engineering, risk refers to the potential for undesired outcomes affecting system design, whereas in cybersecurity, it pertains to potential loss or harm from threats. This distinction is reflected in the workflows discussed in subsequent sections.

A set of safety and security processes is then defined and prioritised based on input from the risk management strategy. Operational risks and gaps identified by the system operator are passed on to the Safety, Security, and Quality (SSQ) engineer, who is responsible for resilience and safety design. The SSQ engineer considers both stakeholder requirements and system capabilities to propose suitable solutions. At this point, a decision point (represented by a diamond symbol) involves the system operator, business manager, and SSQ engineer.

They together determine whether the system has achieved adequate resilience. If it has, the information is relayed to the systems engineer to develop a resilient system concept. If not, the process iterates until sufficient resilience is achieved.

Once the resilient system concept is established, the systems engineer incorporates feedback and solutions from the previous decision step, then defines the system in terms of resilience, safety, security, and system-level requirements. These requirements are passed to the SSQ engineer for assessment and treatment, where they conduct risk evaluations and recommend preventive measures. These recommendations enable the systems engineer to refine the system's safety and security controls.

During testing, the systems engineer provides the necessary inputs, including the resilient system definition and quality requirements. A series of tests is carried out across safety, security, and overall system levels collectively referred to as Safety, Security, System (SSS) testing to verify compliance with the defined quality requirements. If areas for improvement are identified, the system and test engineer communicates them to the systems engineer for further refinement.

With reference to Another decision point, marked by a second diamond, involves the systems engineer, SSQ engineer, and the system and test engineer evaluating whether the system meets acceptable quality standards specifically in terms of safety, security, and cyber resilience. If the outcome is positive, the process proceeds to system validation and transition. If not, the resilient system concept is revisited to identify areas needing revision. This represents a concurrent iteration within the methodology.

Upon successful system validation and transition, the goal is to gain assurance. In this context, assurance means confidence that the system is resilient, operates as intended, and stays within the defined time and cost constraints. Assurance also confirms that the system delivers the required capabilities to stakeholders in its operational environment. The final decision point concerns acceptable transition: agreement between the stakeholder and systems engineer that the system, as transitioned, meets the required capabilities and quality standards. If this agreement is reached, a baseline cyber resilient system is established. If not, the process must return to the existing system concept due to misalignments in capabilities and qualities.

Throughout the meta level methodology, specific roles and responsibilities are defined. Based on our experience, the following key roles are identified: Systems Engineer, Business Manager, System Operator/Expert, Safety, Security & Quality (SSQ) Engineer, and Systems & Test Engineer. In other domains, alternative roles such as Architect or Product Owner may take on responsibilities typically assigned to the Systems Engineer or Business Manager. The IEC 62443 standard also outlines core roles including but not limited to Asset Owner, Product Supplier, and Service Provider (including integration and maintenance service providers) which may be relevant depending on the business context. These roles can vary depending on organisational needs and domain-specific practices [7] [13].

The next section will outline the step-based workflow and how relevant standards guide the development of these workflows.

2.2 Step based workflow

At this level, each block from the meta level is broken down to define the necessary steps, inputs, and outputs required to achieve resilience. The relationships between blocks are clarified, actions are defined, and the iterative process is explained.

The **first** iterative loop explores the problem space of an existing constituent system intended to support resilience at the SoS level. Risks are assessed for potential operational and business impacts. The outputs include a defined problem scope and a resilience construct (comprising goals, capabilities, and effectiveness measures), potentially including a system architecture based on the current concept. Any new capabilities must be balanced against the operational concept and associated risks.

The **second** loop focuses on the solution space and concludes with a decision on quality assurance. Safety and security assessments must provide sufficient confidence that the system will perform within its defined constraints. Where uncertainty remains especially regarding unintended emergent behaviour additional tests and verifications may be required.

The **third** loop validates the solution and prepares it for integration into the wider SoS. This results either in a transition of ownership (with associated risks updated), or a revision of scope regarding the constituent system. The systems engineer may then revisit the existing system concept or baseline the resilient concept to continue SoS development.

These three iterative loops, along with their recursive application at the SoS level, align with recognised systems and software engineering standards. The methodology supports the integration of resilience into existing constituent systems within a system of systems.

2.2.1 SoS Capability Engineering to System Concept

Figure 5: SoS capability engineering to system concept at level 2.

The alignment with the Business/Mission Analysis process outlined in ISO 15288. Its purpose is to define the goals, required (or additional) organisational capabilities, and initial requirements specifically, measures of effectiveness (MOEs) for achieving resilience at the System of Systems (SoS) level. MOEs are criteria that evaluate how well a mission objective is achieved under given conditions. These are critical from the stakeholder's perspective, as they provide the basis for assessing the quality of a proposed solution [14].

Often, this process involves revising or updating a high-level operational concept. Enhancing resilience may require changes to how existing constituent systems are operated, modified, or upgraded.

For example, in the context of Figure 3, the mission goal could be commuting from point A to B. A corresponding business goal or organisational capability could be to offer a transport service that enhances the resilience of this journey. An operational capability could involve supporting the driver in overcoming disruptions and selecting the most resilient route. Requirements for ‘providing a resilient route’ would include mitigating threats that prevent the journey from being successfully completed.

2.2.2 Existing System Concept

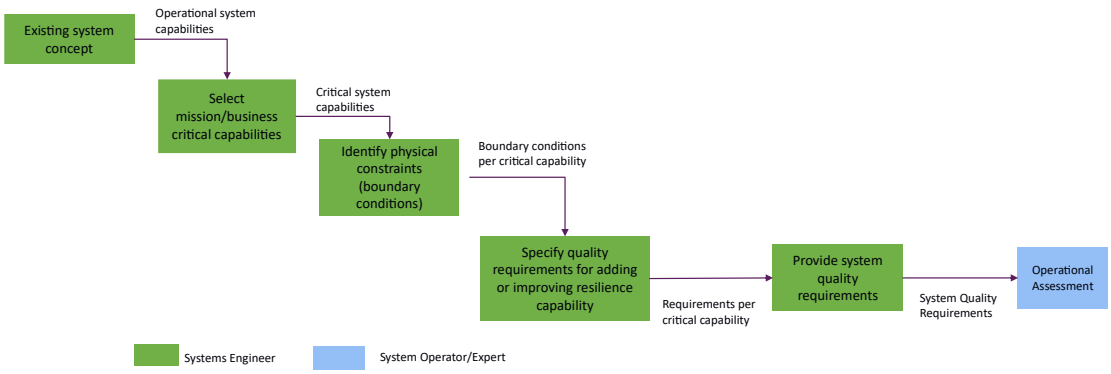

Figure 6: Existing system concept at level 2.

This workflow aligns with the *Stakeholder needs and requirements definition* process from ISO 15288. Its purpose is to identify the needs and requirements of all stakeholders involved in upgrading or modifying an existing system.

This often involves revising the current system concept. Enhancing system resilience may impact both how the system is operated (Operations Concept a.k.a. OpsCon) and how it is

modified or upgraded (Concept of Operations a.k.a. ConOps). The focus should remain on the critical system capabilities that most directly support mission or business objectives.

Referring to the example in Figure 3, if ‘providing a resilient route’ is the required operational capability at the SoS level (e.g., a vehicle and its driver), then an enabling system capability might be the delivery of up-to-date threat information via the vehicle’s infotainment system. In this case, the existing entertainment system would require an upgrade to prioritise and deliver these messages while driving a key boundary condition. Requirements might include appropriate sound levels and possibly an acknowledgement message from the driver. These are examples of system quality requirements designed to support resilience-related functions.

2.2.3 Risk Management Strategy

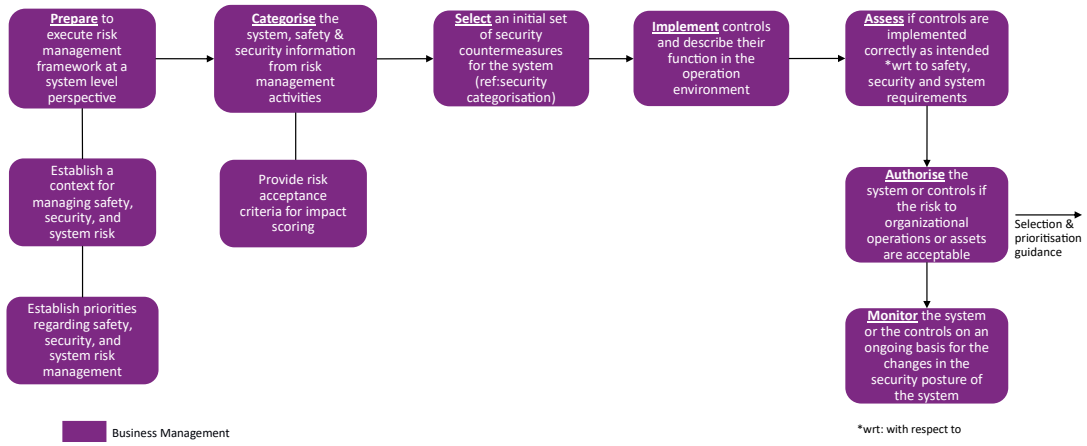

Figure 7: Risk management strategy at level 2.

In this risk management strategy, depicted in Figure 7, NIST 800-37 Revision 2, which outlines the steps and structure of a risk management framework [11]. The framework emphasises stakeholder needs and highlights how an organisation's approach to quality controls encompassing safety, security, and system considerations affects the specification of requirements within systems engineering. Requirements are managed at an appropriate level of granularity to influence the system life cycle, while also considering potential negative impacts on the system, its operational environment, and the organisation's business objectives.

The main steps of the NIST risk management framework as shown in Figure 7are:

- Prepare
- Categorise
- Select
- Implement
- Assess
- Authorise
- Monitor

Depending on the domain, some organisations may adopt the cybersecurity framework, which consists of identify, protect, detect, respond, recover and govern [15]. While this framework offers a starting point through its profiles, the NIST risk management framework provides further guidance on implementing security controls and identifying where risk management supports different stages of the methodology.

It is also important to account for changes in the operational environment, economic conditions, regulations, and the system of systems context. These factors may influence the suitability and customisation of a risk management strategy for a given organisation.

Finally, the risk management strategy also informs the validation stage of the system life cycle, which will be discussed in the *System Validation and Transition* section.

2.2.4 Operational Assessment

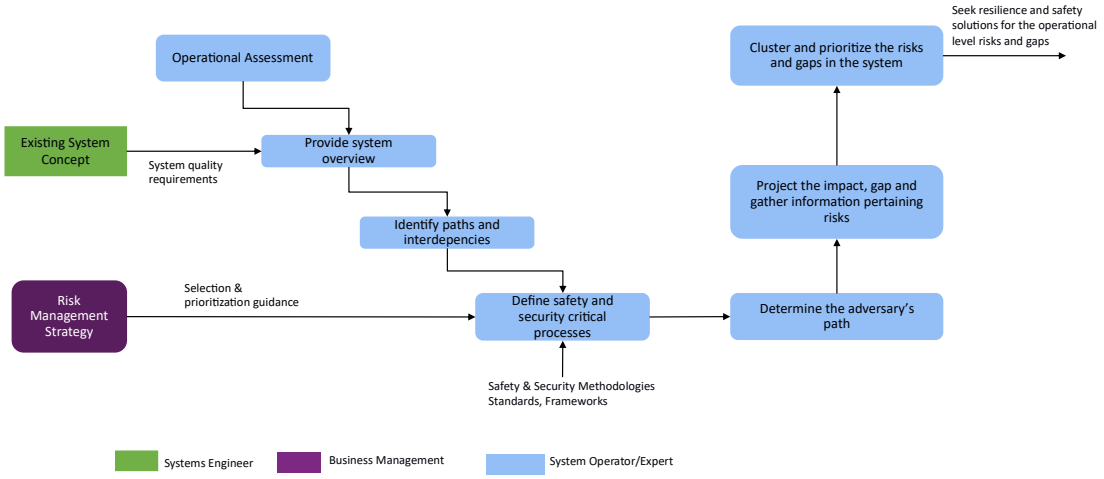

Figure 8: Operational assessment at level 2.

This operational assessment workflow is inspired by the Consequence-Driven Cyber-Informed Engineering Framework, provided by Idaho National Laboratory [16]. The cyber-informed engineering approach assists system operators in identifying critical system points that may be vulnerable to cyberattacks.

During the operational assessment phase, the system operator reviews the system overview (developed by the systems engineer during the existing system concept phase) and identifies system paths and interdependencies. It is essential to define safety and security-critical processes at this stage.

To support this, methodologies such as System-Theoretic Process Analysis (STPA), its security-focused variant STPA-Sec [17], the MITRE Cyber Resiliency Engineering Framework (CREF), and other domain-specific best practices are employed.

The risk management strategy contributes inputs by guiding the selection and prioritisation of critical processes from both stakeholder and system perspectives. When combined with safety and security methodologies, these inputs help identify potential adversarial paths and system vulnerabilities. The resulting insights can be clustered and prioritised based on the system operator's view of risk.

The next step involves identifying appropriate resilience and safety solutions for these operational-level risks and gaps, which will be detailed in the following section.

2.2.5 Resilience Construct

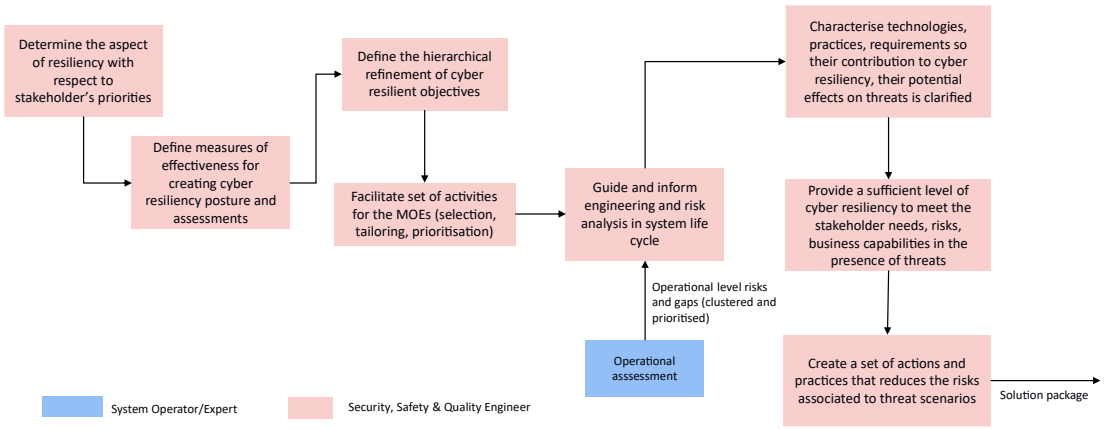

Figure 9: Resilience construct at level 2.

The resilience construct workflow aligns with the *Cyber resilience Engineering Framework* outlined in NIST 800-160 Vol. 2 Rev. 1 [10]. This framework provides guidance on integrating stakeholder priorities into the systems engineering life cycle and is designed to be used alongside ISO 15288. Security-related activities and tasks are incorporated as supplementary elements within the life cycle process. The construct focuses on operational resilience, validation through measures of effectiveness (MOEs), and how these translate into systems engineering activities that contribute to overall cyber resilience.

The framework also offers guidance for addressing technical and operational threats in the system's environment. As such, input from the system operator regarding operational-level risks and gaps is essential to inform engineering decisions and risk analysis throughout the life cycle.

As the methodology is domain-agnostic, the steps are designed to be adaptable. Any of the 30 processes defined in the MITRE CREF may be applied depending on the domain in question. Nevertheless, the resilience construct outlined here provides critical steps for preparing the system to accommodate changes in the operational environment, organisational capabilities, or the broader System of Systems (SoS) context. These changes can affect system resilience and the traceability of design modifications.

To ensure alignment, a concurrent iteration is carried out in meta level methodology. During this stage, the SSQ engineer, business manager, and system operator must reach consensus on the necessary steps before the solution package is handed over to the systems engineer for implementation.

2.2.6 Resilient System Concept

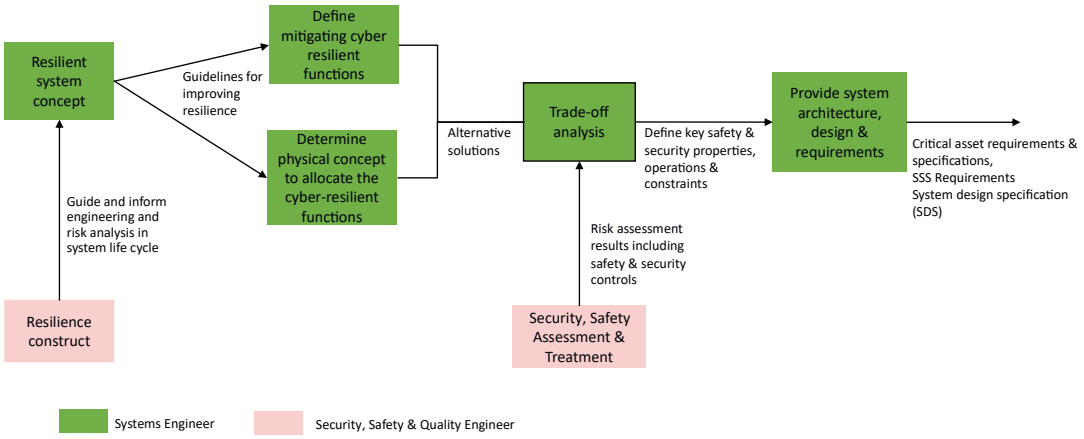

Figure 10: Resilient system concept at level 2

The *resilient system concept* represents the asset to be developed. In systems engineering, an asset refers to a resource, component, or entity, whereas in cybersecurity it includes anything of value that must be protected from threats and vulnerabilities. The workflow in Figure 10 is aligned with ISO 15288 processes, including *System Architecture Definition*, *System Design Definition*, *System Analysis*, and *System Requirements Definition*. The objective is to define a viable solution that fits the identified problem and aligns with the system architecture as part of the resilience construct.

The workflow begins by defining mitigating functions necessary for achieving cyber resilient system capabilities. This involves breaking down and identifying system elements or components that support these functions. Functional and physical decomposition should occur in parallel and may lead to multiple alternative solutions. A trade-off analysis is then conducted to select the most viable option, considering other critical quality attributes such as safety and security. The workflow concludes with the definition of the system's architecture, design, and requirements.

For example, referring to Figure 3, if the infotainment system is the resilient system concept, and its intended function is to suggest route changes, this can be broken down into sub-functions such as detecting route blockages and warning the driver. Supporting components may include sensors, speakers, and displays. These functions must be constrained by both safety and security requirements. For instance, information must be trustworthy (security) and presented in a way that allows the driver to respond safely and without distraction (safety). Alternative implementations could include mobile or fixed in-vehicle solutions.

2.2.7 Security, Safety Assessment & Treatment

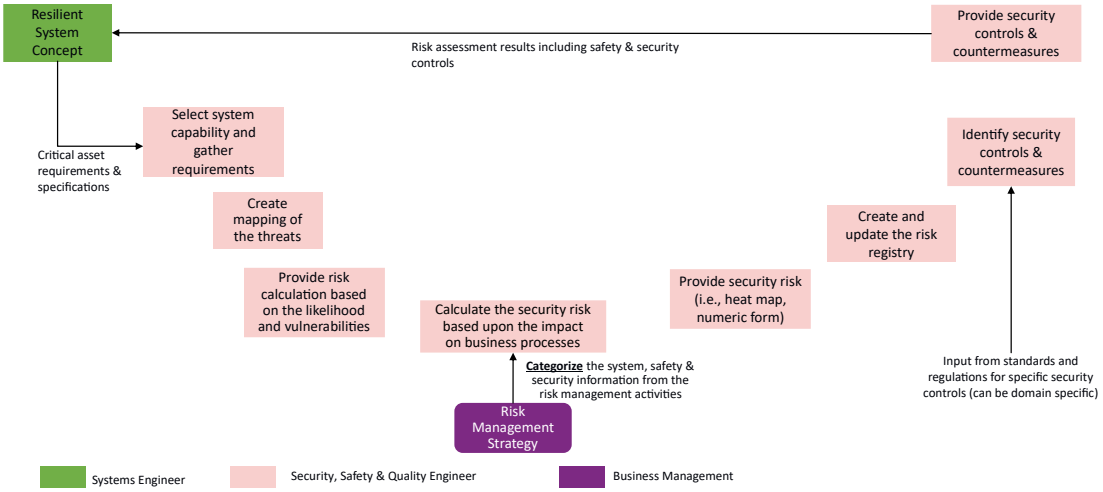

Figure 11: Safety, security assessment and treatment at level 2.

In figure 11, the safety and security assessment begins with the Resilience System Concept (see Section 2.2.6). A specific system capability and its corresponding requirements are selected. Once the relevant (sub-)system is identified, a detailed threat mapping is carried out using the organisation's preferred threat modelling techniques [18] The subsequent steps involve the Safety, Security, and Quality (SSQ) engineer performing risk calculations.

From the NIST definitions, [19] a cyber threat is any event or circumstance that adversely affects an organisation's operations such as its mission, functions, image, or reputation or its assets, through a system via unauthorised access, destruction, disclosure, modification of information, or denial of service. Cyber threats are a core component of risk analysis. In this context, a *vulnerability* is a weakness within an information system or its security that can be exploited by a threat actor or vector.

Business impact analysis is used to assess the effects of operational disruptions. This analysis evaluates the impact of a potential cyber incident on business functions and workflows. The resulting impact score is then used in the calculation of *cybersecurity risk*, defined as the product of likelihood (informed by vulnerabilities and threats) and business impact [20]. This approach demonstrates the synergy between systems engineering and cybersecurity perspectives on risk. The risk output may be visualised as a heat map (e.g., low-medium-high risk shown in green, yellow, and red respectively) or as a numerical value, depending on organisational preferences.

Finally, appropriate safety and security controls are identified and returned to the *Resilient System Concept* workflow, ensuring traceability and alignment with the assessed risks.

2.2.8 Security, Safety, System (SSS) Test & Verification

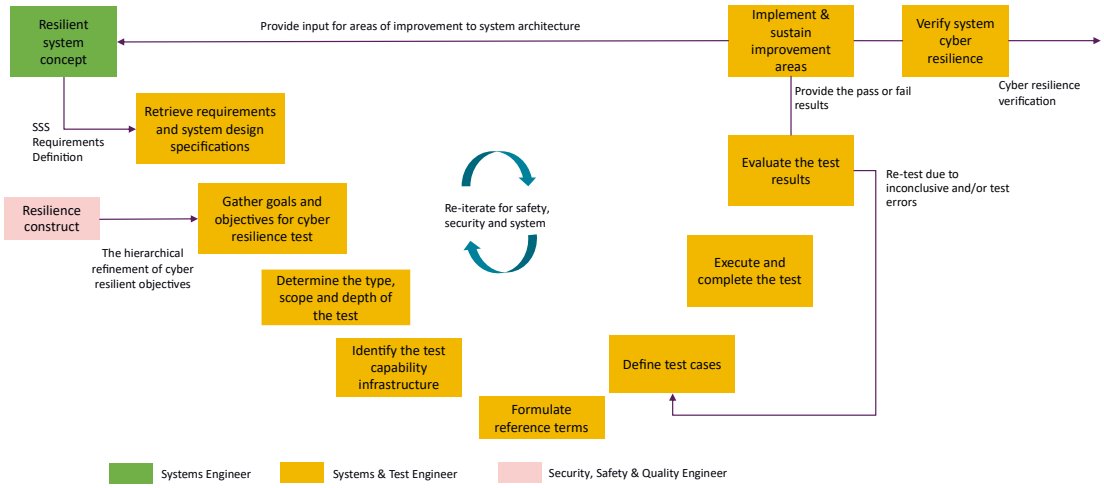

Figure 12: Security, safety and system (SSS) test and verification at level 2.

The *Security, Safety, and System (SSS) Test and Verification* workflow provides an iterative methodology in which testing is carried out across three quality dimensions: security, safety, and system-level performance. Regardless of the test type, clear requirements, goals, and objectives must first be established to define the scope, type, and depth of testing needed.

In ISO 15288 [8], these activities are typically addressed during the *Quality Assurance* and Implementation phases. ISO 829-2008, section 10, introduces the Master Test Plan (MTP) [9], while IEC 62443 includes dedicated guidelines for security testing and best practices [21]. These standards inspired us to create our workflow in the following manner:

- The *systems engineer* provides the verification requirements.
- The *SSQ engineer* contributes cyber resilience objectives from their workflow.
- The *capability infrastructure* is assessed to determine feasibility in terms of cost, time, scheduling, and risk since in-depth testing can be resource intensive.

Once the testing infrastructure is confirmed, reference terms and test cases are defined and executed. If results are inconclusive or test errors occur, the test cases are reviewed and repeated until definitive pass/fail outcomes are achieved. These results feed into the decision-making process for the systems engineer either prompting updates in the second loop of the meta level methodology or enabling progression in the cyber resilience verification process. Safety testing is typically performed alongside security testing, with an emphasis on system vulnerabilities, resilience to threats, and response to attacks already addressed in the first loop of the meta level methodology.

This integrated approach has been cross-checked against the security testing guidance from the National Cyber Security Centre (NCSC) of the Netherlands, ensuring that all relevant quality aspects are accounted for within the cyber resilience workflow [22].

2.2.9 System Validation & Transition

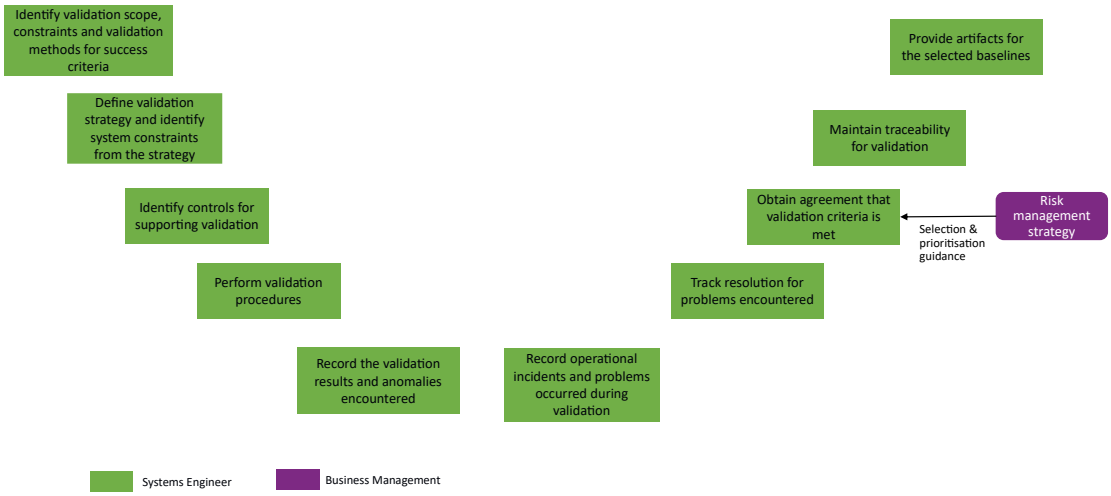

Figure 13: System validation and transition at level 2.

System Validation & Transition (SVT) is a critical phase in engineering cyber resilient high-tech systems. It provides assurance that systems meet their design specifications and perform reliably under real-world conditions, including exposure to potential cyber threats. However, validation also requires that the system meets stakeholder needs and expectations. This workflow includes rigorous validation steps to ensure that security controls are effective, resilience measures are properly implemented, and an agreement is reached with stakeholders before finalising the system as the baseline cyber resilient solution.

Assurance activities in this phase confirm that the system can maintain availability, integrity, and functionality despite evolving cyber challenges. This gives stakeholders confidence in the system's resilience, adaptability, and ability to recover from disruptions.
The workflow is primarily based on the *Transition* and *Validation* processes from ISO 15288. The transition process ensures a smooth progression from development to operational deployment, while the validation process confirms that system requirements are met and that the system performs as intended. NIST 800-12 further supports this phase, particularly in areas of security testing, accreditation, and user acceptance [12].

Stakeholder agreement, including input from business management, is crucial during validation. It is possible that the initially proposed design may no longer be feasible. For example, referencing the Level 0 example: a fixed in-car infotainment system may prove too costly or time-consuming to develop, whereas a mobile application could provide a faster, more secure, and safer alternative prompting a reassessment of the problem domain.

Context also plays a key role. A solution may be acceptable in one context but not in another. Using the car example, a vehicle designed for city driving may not meet the requirements for transporting a high-profile individual such as a head of state. While the underlying functionality might remain the same, the operational context can render the solution inadequate. In such cases, reputational damage, financial loss, and disruption to mission continuity are real risks if the system fails to deliver its intended qualities.

2.3 Baseline Cyber resilient System

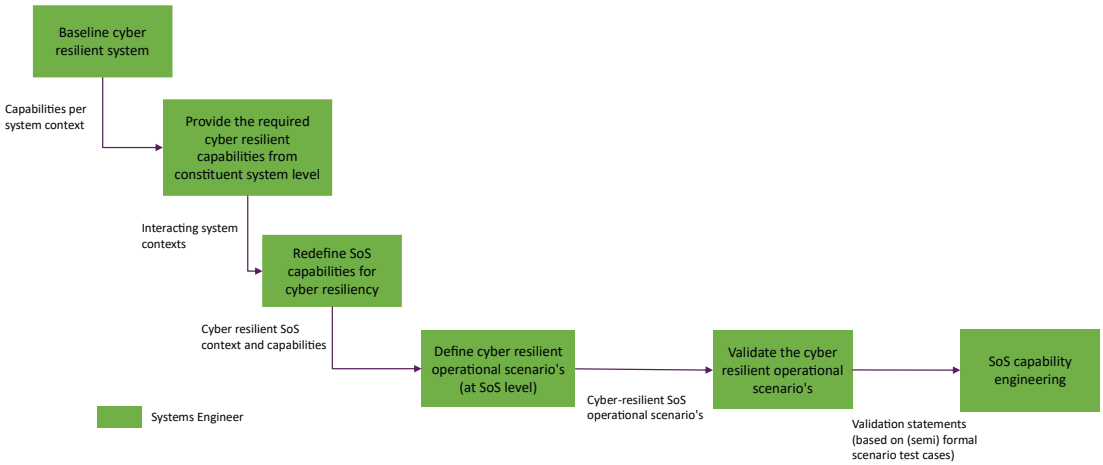

Figure 14: Baseline cyber resilient system at level 2.

Once the solution is defined and accepted, the new resilience capability of a constituent system can be baselined as a reference for further development, realisation, and deployment at the System of Systems (SoS) level. This step aligns with *System Analysis* and *Validation* processes from ISO 15288, applied at the SoS level. Its purpose is to validate that the combination of resilient system concepts contributes to a coherent and effective capability across the SoS.

As each constituent system is validated, the associated risks for developing the resilient SoS are updated. A validation statement indicates that a part of the broader problem has been resolved, and risk ownership is then transferred to other constituent systems yet to be developed or upgraded.

For example, referring to Figure 3: if the *entertainment system* is replaced with a fixed *infotainment system* in the car, the *data system* may require modifications to handle high-priority messages such as warnings or alarms and possibly control functionalities (e.g., switching operating modes of the infotainment system). These features support the driver in selecting resilient routes. To enable this, both systems may need to interact directly with the driver.

By integrating the operational scenarios from the entertainment and data systems, the expanded or combined capability at the vehicle level can then be redefined and validated to support overall resilience.

2.4 Domain Specific Workflow Changes

In the sub-sections of Section 2.2, we presented an overview of the workflows and how roles and responsibilities contribute across them. The workflows are designed to be domain-agnostic; however, when applied to specific domains, we anticipate changes at a minimum in the meta level methodology.

Depending on the system context (i.e., the problem space), alternative solutions may differ in effectiveness. As such, domain-specific reference architectures may be incorporated into the resilience construct to guide the intended use of constituent systems. These reference architectures should offer sufficient detail to support the development of system architectures within the resilient system concept.

Because the methodology is applied iteratively to build cyber resilience at the SoS level, parts of the workflow may be automated to achieve stakeholder-defined qualities within a specific domain. This requires close alignment between business goals and system goals often informed by the reference architecture. In domain-specific contexts, this relationship can become more complex, potentially requiring additional workflows to support the desired level of automation.

Moreover, domain-specific standards and enterprise-level risk management strategies may introduce further steps beyond those included in the agnostic workflows. Examples of relevant standards include:

- **IEC 30141** – Reference architecture for the Internet of Things
- **ISO/IEC 27030** – Guidelines for IoT security
- **IEC 63168** – IoT system reference architecture (currently under development or in regional draft stages)

When moving towards domain specificity, the focus shifts from technical processes to organisational project-enabling processes, such as maintenance, disposal, infrastructure management, portfolio management, and knowledge management [8]. These transitions may necessitate significant changes in workflows beyond those prescribed in the meta level methodology.

The **IEC 62443** standard set, for example, includes detailed guidance for Operational Technology (OT) security and Internet of Things (IoT) security. It defines security programme requirements for various roles (e.g., asset owners, service providers), and provides system-level risk assessments, product-level cybersecurity, and component-level security for the Industrial Automation and Control Systems (IACS) domain. Organisations within the supply chain and industrial automation sectors may benefit significantly from this suite of standards.

To support practical application, we have included a few non-domain-specific level 3 examples highlighting high-level steps for tool and method execution in **Appendix A**.

3 On-going evaluation of the methodology by the industry

In the previous sections, we presented a domain-agnostic methodology that bridges systems engineering and cybersecurity practices. This state-of-practice approach demonstrates the value of integrating cyber resilience into the design process of cyber-physical systems, with a focus on supporting the Dutch industry. Drawing from established systems engineering principles, relevant standards, and frameworks, the methodology provides clear steps to enhance resilience, traceability, and role clarity ultimately contributing to improved business continuity and cyber resilient system development.

Within TNO-ESI's security portfolio, the **SecureArch** project is ongoing in collaboration with a partner from the material handling, logistics, and industrial automation sector. This project explores security risk assessments and trade-offs between various system quality attributes. In parallel, the **INTERSCT** project engages with Dutch industry stakeholders through regular cybersecurity round-table sessions. These discussions have highlighted the industry's uncertainty about how to apply standards effectively, create cyber resilience, and manage cyber-related risks especially in systems that include third-party components. The feedback has been instrumental in refining our methodology and improving the workflows between the blocks of the meta level methodology. Appendix D provides an updated inventory of standards, frameworks, and guidelines, based on this on-going evaluation. Appendix E presents insights from the initial application of the methodology that demonstrate its *relevance* and practical *applicability*, while also informing future developments.

Our approach is adaptable to specific domains and applications relevant to the Dutch market. The SecureArch project validates our understanding of industry needs and demonstrates how our methodology delivers tangible value. In this context, the customer typically acts as the Asset Owner (owner of the SoS), while the partner company plays dual roles as Product Supplier and Service Supplier (for integration and maintenance). Constituent systems or products that make up the SoS may be developed, delivered, or supported by the company or by third parties. Mapping these roles across organisations leads to a corresponding transfer of risk ownership. As shown in Figure 2, the life cycle stages may vary per domain, though this paper focuses on the concept phase, with operational and maintenance aspects considered domain specific. Future work should demonstrate the application of this methodology in a concrete industry use case.

We extend our sincere thanks to our project partners and round-table participants for their valuable input. Their insights and critical review have significantly enhanced the maturity of our methodology. We deeply appreciate their time and support, which reinforces our belief that this approach has the potential to both innovate and add measurable value to the Dutch industrial landscape.

4 References

[1] IBM, “IBM,” 2025. [Online]. Available: https://www.ibm.com/topics/cyber-resilience. [Accessed 2 January 2025].

[2] TNO, 2025. [Online]. Available: https://365tno.sharepoint.com/teams/T99131/TeamDocuments/Team/Deliverables/Management/2025/Impact%20pathway/Impact%20pathway%20ERP%20Cyber-secure%20systems%20by%20design.pptx?web=1.

[3] R. Haberfellner, O. de Weck, E. Fricke and S. Vössner, Systems Engineering, Cham: Springer International Publishing, 2019.

[4] R. Dove, K. Willett, T. McDermott, H. Dunlap, D. P. MacNamara and C. Ocker, “Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts,” in *INCOSE International Symposium*, Honolulu, HI, 2021.

[5] INCOSE, “SE Vision 2035,” 2023. [Online]. Available: https://www.incose.org/2023_redesign/publications/se-vision-2035.

[6] P. Beling, “Cyber Security Requirements Methodology: Tools & Transition,” 19 November 2019. [Online]. Available: https://sercuarc.org/wp-content/uploads/2019/12/Track3_1_Beling_CyberSecurity-Reqs-Method-SSRR-2019.v1.0.pdf. [Accessed 14 April 2025].

[7] ISA, “ISA/IEC 62443 Series of Standards,” ISA.ORG, 2 March 2020. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 1 April 2025].

[8] I. Society, “ISO,” May 2023. [Online]. Available: https://www.iso.org/standard/81702.html. [Accessed 15 January 2025].

[9] I.-. S. S. Board, “IEEE,” 27 March 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4578383. [Accessed 23 March 2025].

[10] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau and R. McQuaid, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” NIST, December 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf. [Accessed 14 January 2025].

[11] W. Ross and W. Copan, “NIST 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations,” NIST, December 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [Accessed 3 March 2025].

[12] M. Nieles, K. Dempsey and V. Y. Pillitteri, “NIST 800-12- Rev 1 An Introduction to Information Security,” NIST, June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. [Accessed 2 April 2025].

[13] M. Müller, “IEC 62443 Industrial Security Standards- An Introduction to the Framework,” TUVSUD, 20 July 2020. [Online]. Available: https://www.tuvsud.com/en-za/-/media/regions/in/pdf-files/resource-center/whitepapers/tuv-sud-iec-62443-industrial-security-standards.pdf. [Accessed 29 March 2025].

[14] D. Kaslow, B. Ayres, P. T. Cahill and L. Hart, “A Model Based Systems Egnineering Approach for Technical Measurement with Application to a CubeSat,” INCOSE, 2018. [Online]. Available: https://www.incose.org/docs/default-source/space-systems-working-group/sswg_csrm_papers_to_display/2018-ieee-aero-conf---mbse-approach-for-technical-measurement-with-application-to-a-cubesat.pdf?sfvrsn=7f6593c6_4. [Accessed 10 February 2025].

[15] NIST, “Cybersecurity Framework,” NIST CSF, 8 April 2018. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 5 Feb 2025].

[16] S. Cramer, R. Helton, R. Smith and C. St. Michel, “Idaho National Laboratory,” U.S. Department of Energy National Laboratory, June 2023. [Online]. Available: https://inl.gov/content/uploads/2023/06/Consequence-driven-Cyber-informed-Engineering.pdf. [Accessed 13 March 2025].

[17] T. Consortium, “Solutions for end-to-end safety and performance for distributed CPS,” TRANSACT, 2 December 2024. [Online]. Available: https://transact-ecsel.eu/wp-content/uploads/2024/05/TRANSACT-D33-D3.5-Solutions-for-end-to-end-safety-and-performance-for-distributed-CPS-v2.pdf. [Accessed 3 April 2025].

[18] L. Conklin, “Threat Modelling Process,” OWASP, 2025. [Online]. Available: https://owasp.org/www-community/Threat_Modeling_Process. [Accessed 7 April 2025].

[19] NIST, “NIST Computer Security Resource Center,” NIST, [Online]. Available: https://csrc.nist.gov/glossary/. [Accessed 24 April 2025].

[20] NIST, “NIST Cyber Risk Scoring,” February 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/nist-cyber-risk-scoring-crs-program-overview/images-media/NIST%20Cyber%20Risk%20Scoring%20(CRS)%20-%20Program%20Overview.pdf. [Accessed 24 April 2025].

[21] ISA, “ISA-62443-4-1-2018, Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements,” ISA, 1 April 2018. [Online]. Available: https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au. [Accessed April 5 2025].

[22] NCSC, “Security Testing White Paper,” Nationaal Cyber Security Centrum, 30 March 2020. [Online]. Available: https://english.ncsc.nl/binaries/ncsc-en/documenten/whitesheets/2020/march/30/security-testing-white-paper/Security+testing+White+Paper.pdf. [Accessed 12 March 2025].

[23] I. Society, “ISO 15288 Systems and software engineering,” May 2023. [Online]. Available: https://www.iso.org/standard/81702.html. [Accessed 15 January 2025].

[24] ISO, “2700 series family,” 2025. [Online]. Available: https://www.iso.org/search.html?PROD_isoorg_en%5Bquery%5D=27000. [Accessed 5 March 2025].

[25] ISO, “IEC 30141 Standard,” August 2024. [Online]. Available: https://www.iso.org/standard/88800.html. [Accessed 19 February 2025].

[26] IEC, “IEC 63168,” March 2022. [Online]. Available: https://www.vde-verlag.de/standards/1701763/e-din-iec-63168-2-vde-0750-34-2-2022-03.html. [Accessed 15 March 2025].

[27] E. R. Agency, “Guide for application of the CSM Regulation,” 1 June 2009. [Online]. Available: https://www.era.europa.eu/system/files/2022-11/Guide%20for%20the%20application%20of%20the%20Common%20Safety%20Methods%20on%20risk%20assessment%20%28EN%29.pdf?t=1751549664. [Accessed 2 April 2025].

[28] O. M. G. (OMG), “Risk Analyssi and Assessment Modeling Language (RAAML) Libraries and Profiles,” December 2022. [Online]. Available: https://www.omg.org/spec/RAAML/1.0/PDF. [Accessed 22 February 2025].

[29] O. M. G. (OMG), “System Profile for Effective Cyber Threat-based Risk Asssessments (SPECTRA) version 1.0,” April 2025. [Online]. Available: https://www.omg.org/spec/SPECTRA/1.0/Beta1/Volume1/PDF. [Accessed 3 April 2025].

[30] MIT, “Introduction to STPA for Security (STPA-SEC),” April 2013. [Online]. Available: https://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/Basic_STPA_Tutorial1.pdf. [Accessed 10 February 2025].

[31] S. Acur, S. Das, B. van der Leeuw, A. Vasenev and P. Goosen, “Cyber resilient system design methodology,” 2025. [Online]. Available: https://ris-data.tno.nl/bibliotheek/sv-015068/TNO/Rapporten/2025/TNO-2025-R10875.pdf. [Accessed 29 July 2025].

[32] INTERSCT, “Towards an Internet of Secure Things,” [Online]. Available: https://intersct.nl/. [Accessed 29 July 2025].

[33] ISA, “ISA/IEC 62443 Series of Standards,” 2025. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 29 July 2025].

5 Appendix A : Level 3

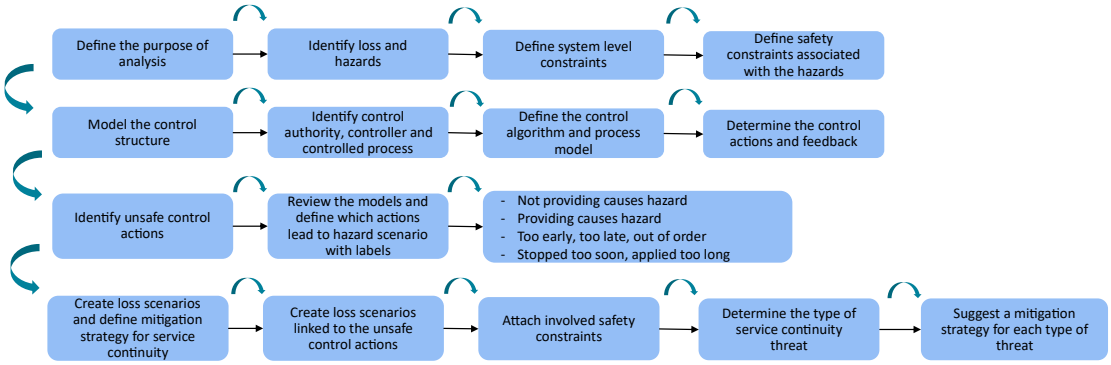

Figure 15: Operational assessment at level 3 using STPA.

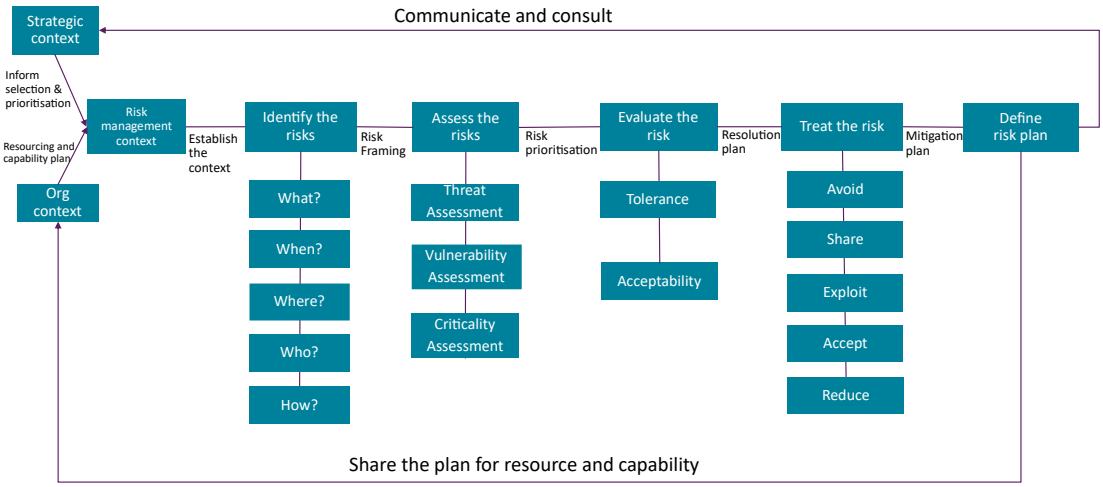

Figure 16: Risk management strategy descriptions at level 3.

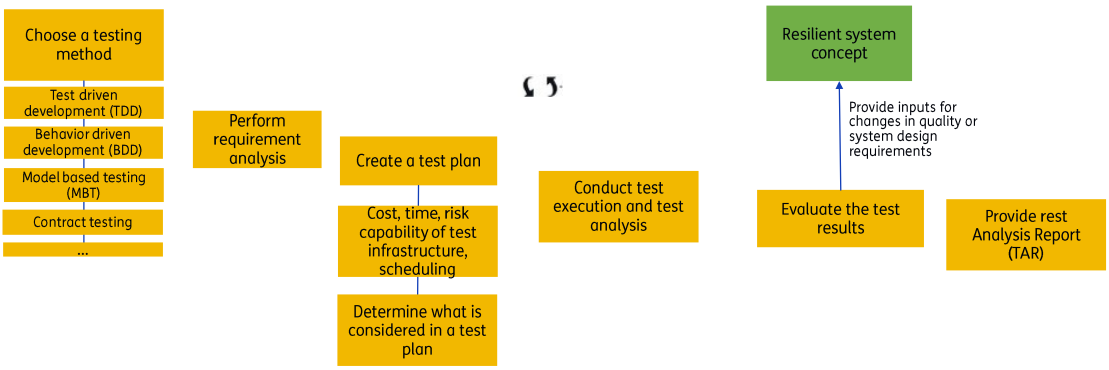

Figure 17: System testing at level 3 descriptions.

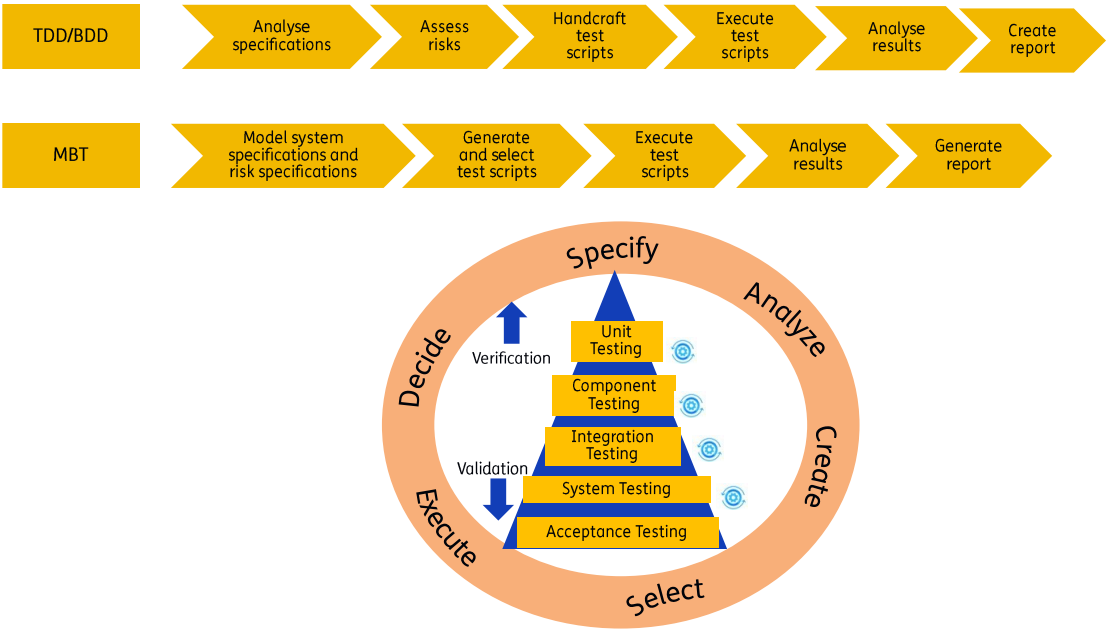

Figure 18: System testing at level 3 descriptions.

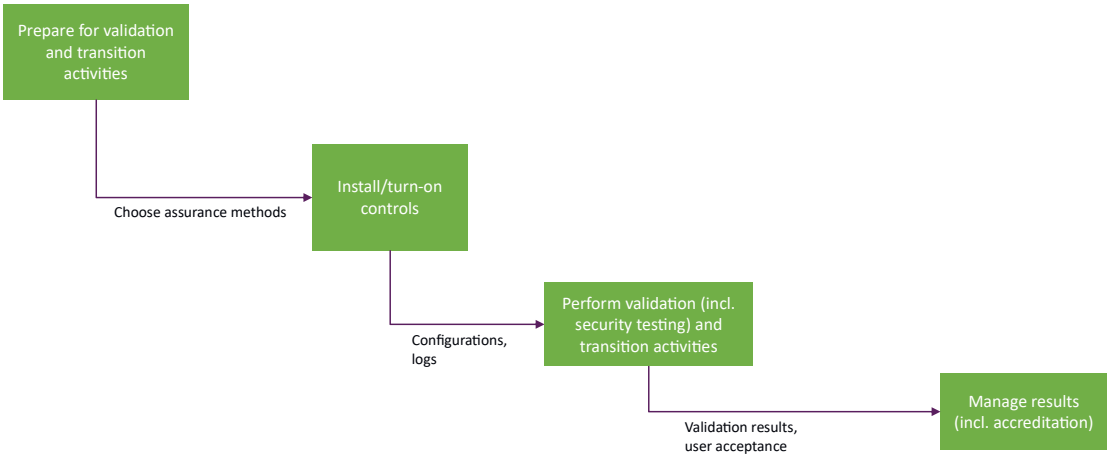

Figure 19: System validation and transition at level 3 descriptions.

6 Appendix B : Glossary

activity	Set of cohesive tasks of a process. [ISO 15288:2023]
adversity	The conditions that can cause a loss of assets (e.g., threats, attacks, vulnerabilities, hazards, disruptions, and exposures). [NIST 800-160v1r1]
architecture	Fundamental concepts or properties of a system in its environment and governing principles for the realisation and evolution of this system and its related life cycle processes . [ISO 15288:2023]
architecture (system)	Fundamental concepts or properties related to a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution. [NIST 800-160v1r1]
aspect	The parts, features, and characteristics used to describe, consider, interpret, or assess something. [NIST 800-160v1r1]
assurance	Grounds for justified confidence that a claim has been or will be achieved. [NIST 800-160v1r1]
availability	Property of being accessible and usable on demand by an authorised entity. [NIST 800-160v1r1]
baseline	Formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle. [ISO 15288:2023]
complex system	A system in which there are non-trivial relationships between cause and effect: each effect may be due to multiple causes; each cause may contribute to multiple effects; causes and effects may be related as feedback loops, both positive and negative; and cause-effect chains are cyclic and highly entangled rather than linear and separable. [NIST 800-160v1r1]
constraints	Limitation on the system, its design, its implementation, or the process used to develop or modify a system. [NIST 800-160v1r1]
control	Purposeful action on or within a process to meet specified objectives. The mechanism that achieves the action. [NIST 800-160v1r1]
customer	Organisation or person that receives a product or service. [ISO 15288:2023]
cyber resiliency	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. [NIST 800-160v2r1]

cyber risk	The risk of depending on cyber resources (i.e., the risk of depending on a system or system elements that exist in or intermittently have a presence in cyberspace). [NIST 800-160v2r1]
cyber-physical system	A system integrating computation with physical processes whose behaviour is defined by both the computational (digital and other forms) and the physical parts of the system. [NIST 800-160v1r1]
cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks. [NIST 800-160v2r1]
design	Specification of system elements and their relationships, that is sufficiently complete to support a compliant implementation of the architecture. [ISO 15288:2023]
domain	A set of elements, data, resources, and functions that share a commonality in combinations of (1) roles supported, (2) rules governing their use, and (3) protection needs. [NIST 800-160v1r1]
emergence	The behaviours and outcomes that result from how individual system elements compose to form the system as a whole. [NIST 800-160v1r1]
environment	<System> context determining the setting and circumstances of all influences upon a system. [ISO 15288:2023]
information	Knowledge that is exchangeable amongst users, about things, facts, concepts, and so on, in a universe of discourse. [NIST 800-160v1r1]
integrity	Quality of being complete and unaltered. [NIST 800-160v1r1]
interface	Wherever two or more logical, physical, or both system elements or software system elements meet and act on or communicate with each other. [NIST 800-160v1r1]
interface	Point at which two or more logical, physical, or both, system elements or software system elements meet and act on or communicate with each other. [ISO 15288:2023]
iteration	<Process> repeating the application of the same process or set of processes on the same level of the system structure. [ISO 15288:2023]
life cycle	Evolution of a system, product, service, project or other human-made entity from conception through retirement. [ISO 15288:2023]
mechanism	A process or system that is used to produce a particular result. [NIST 800-160v1r1]
operational concept	Verbal and graphic statement of an organisation’s assumptions or intent in regard to an operation or series of operations of a specific system or a related set of specific new, existing, or modified systems. [NIST 800-160v1r1]
operational environment	Context determining the setting and circumstance of all influences on a delivered system. [NIST 800-160v1r1]
operator	Individual or organisation that performs the operations of a system. [NIST 800-160v1r1]

organisation	Group of people and facilities with an arrangement of responsibilities, authorities, and relationships. [NIST 800-160v1r1]
outcome	Result of the performance (or non-performance) of a function or process(es). [NIST 800-160v1r1]
problem	Difficulty, uncertainty, or otherwise realised and undesirable event, set of events, condition, or situation that requires investigation and corrective action. [NIST 800-160v1r1]
process	Set of interrelated or interacting activities that use inputs to deliver an intended result. [NIST 800-160v1r1]
product	Output of an organisation that can be produced without any transaction taking place between the organisation and the customer. [ISO 15288:2023]
quality assurance	Part of quality management focused on providing confidence that quality requirements will be fulfilled. [NIST 800-160v1r1]
quality assurance	Part of quality management focused on providing confidence that quality requirements will be fulfilled. [ISO 15288:2023]
requirement	Statement that translates or expresses a need and its associated constraints and conditions. [NIST 800-160v1r1]
requirement	Statement which translates or expresses a need and its associated constraints and conditions. [ISO 15288:2023]
resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. [NIST 800-160v2r1]
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. [NIST 800-160v2r1]
risk analysis	Process to comprehend the nature of risk and to determine the level of risk. [NIST 800-160v2r1]
risk assessment	Overall process of risk identification, risk analysis, and risk evaluation. [NIST 800-160v1r1]
risk management	Coordinated activities to direct and control an organisation with regard to risk. [NIST 800-160v1r1]
safety	Expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered. [ISO 15288:2023]
security	Protection against intentional subversion or forced failure. [ISO 15288:2023]
security risk	The effect of uncertainty on objectives pertaining to asset loss and the associated consequences. [NIST 800-160v1r1]
service	Performance of activities, work, or duties. [NIST 800-160v1r1]

specification	An information item that identifies, in a complete, precise, verifiable manner, the requirements, design, behaviour, or other expected characteristics of a system, service, or process. [NIST 800-160v1r1]
stage	Period within the life cycle of an entity that relates to the state of its description or realisation. [NIST 800-160v1r1]
stakeholder	Individual or organisation having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations. [NIST 800-160v1r1]
supplier	Organisation or an individual that enters into an agreement with the acquirer for the supply of a product or service. [NIST 800-160v1r1]
system	Arrangement of parts or elements that together exhibit a stated behaviour or meaning that the individual constituents do not. [ISO 15288:2023]
system context	The specific system elements, boundaries, interconnections, interactions, and operational environment that define a system. [NIST 800-160v1r1]
system life cycle	Period that begins when a system is conceived and ends when the system is no longer available for use. [NIST 800-160v1r1]
system of systems (SoS)	Set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own. [ISO 15288:2023]
system-of-interest	System whose life cycle is under consideration. [ISO 15288:2023]
systems engineering	Transdisciplinary and integrative approach to enable the successful realisation, use, and retirement of engineered systems using systems principles and concepts and scientific, technological and management methods. [ISO 15288:2023]
threat	Potential cause of unacceptable asset loss and the undesirable consequences or impact of such a loss. [NIST 800-160v1r1]
trade-off	Decision-making actions that select from various requirements and alternative solutions on the basis of net benefit to the stakeholders. [NIST 800-160v1r1]
validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. [ISO 15288:2023]
verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. [ISO 15288:2023]
vulnerability	A weakness that can be exploited or triggered to produce an adverse effect. [NIST 800-160v1r1]

7 Appendix C : Abbreviations

Ref	Reference
CREF	Cyber resiliency engineering framework
CSRM	Cyber security requirements methodology
IACS	Industrial automation and control systems
IoT	Internet of things
MOEs	Measures of effectiveness
MTP	Master Test Plan
OpsCon	Operations concept
OT	Operational technology
Ref	Reference
SE	Systems engineering
SoS	System of systems
SSQ engineer	Safety, security and quality engineer
SSS	Safety, security, system
STPA	System theoretic process analysis
SVT	System validation and transition

8 Appendix D : An inventory of standards, frameworks, and guidelines

8.1 Introduction

As society increasingly relies on tightly integrated cyber-physical systems within systems of systems (SoS), safeguarding data and information against malicious threats becomes critical. For end users to trust these complex, interconnected services, standards play a key role by encapsulating field-tested best practices and enabling resilience, safety, and security at scale.

Standards act as knowledge assets, offering shared definitions, frameworks, and guidance across domains for management, implementation, and certification. They serve the interests of all stakeholders, including manufacturers, users, and regulators.

However, standard development takes time and often lags behind fast-moving technologies. The threat landscape constantly changes by the time a standard is released. While standards provide structure and direction, it's crucial to apply them in a way that strikes a balance between mission continuity and cyber resilience.

8.2 The inventory of standards[1]

Standards serve various purposes and come in many forms. They may be global or local, domain-specific or agnostic, and can define frameworks, certify methods, or provide guidance for security assessments.

The International Organization for Standardization (ISO) develops management standards, often grouped into families such as ISO/IEC 27000 for information security, in collaboration with the International Electrotechnical Commission (IEC). The Institute of Electrical and Electronics Engineers (IEEE) focuses on technology standards, and some, such as ISO/IEEE/IEC 15288 for systems and software life cycles, are supported by all three.

In addition to international bodies, national organisations such as the U.S. National Institute of Standards and Technology (NIST) also develop standards. In Europe, regulations such as the Cyber Resilience Act (CRA) introduce additional cybersecurity requirements for digital products beyond CE marking. Selecting standards often depends on industry adoption and the organisation’s role in the value chain. Using established standards can save time and support collaboration.

[1] This section provides an overall view on standards, (not exhaustive) to include standards (such as IEC, NIST, IEEE etc), proprietary standards (such as OWASP) and guidance documents (such as NCSC, CCE).

This inventory is a representative overview of the standards, frameworks, and guidelines identified throughout developing the cyber-resilient methodology while continuously evaluating (parts of) the methodology by our industry partners.

Source Name	Purpose	Description
ISO/IEC/IEEE 29119 series	IT, Software Testing	This standard was commonly known as IEEE 829, defining templates and structures for test-related documents (test plans, test cases, test logs...). It has been replaced by ISO/IEC/IEEE 29119 series [9].
ISO/IEC/IEEE 15288	Systems Engineering Management	Standard providing a common framework of process descriptions for describing the life cycle of engineered systems, defining a set of processes and associated terminology from an engineering viewpoint. These processes can be applied to systems of interest, their system elements, and to systems of systems. Selected sets of these processes can be applied throughout the stages of a system's life cycle. This is accomplished through the involvement of stakeholders, with the ultimate goal of achieving customer satisfaction [23].
ISO/IEC 27000 series	IT, Information Security Management	Standards for information security management systems (ISMS) and their requirements. Additional best practice in data protection and cyber resilience are covered by more than a dozen standards in the ISO/IEC 27000 family. Together, they enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties. An example here being ISO/IEC 27403:2024 – Cybersecurity, IoT security and privacy, which provides guidelines for IoT domotics. [24].
IEC 30141	IoT, Reference Architecture	This standard provides generic, top down IoT reference architecture framework including conceptual, functional and implementation patterns in architecting [25].
IEC 62443	OT, Technology Security Management	Standards for security of industrial automation and control systems (IACS). IT standards are not appropriate for IACS and other OT (operational technology) environments. For example, they have different performance and availability requirements, and equipment lifetime. Moreover, cyber-attacks on IT systems have essentially economic consequences, while cyber-attacks on critical infrastructure can have severe environmental or public-health consequences, that threatens lives [21].

IEC 63168 series	IoT, Safety Engineering Management	This standard is work in progress; it has four parts that focus on safety requirements for IoT devices particularly in connected home environments. First part provides general requirements for design and development, second part is guidelines on hazard analysis, risk assessment and System in Loop (SIL). Third part is on product development requirements and last part is on functional safety requirements [26].
Consequence-driven Cyber-Informed Engineering (CCE)	Security Engineering Management	Idaho National Laboratory created this framework to protect critical infrastructure systems such as power grids, water systems. It starts with identifying the worst-case scenarios then identifying and eliminating pathways leading to catastrophic outcomes [16].
Common Safety Method for Risk Evaluation and Assessment (CSM-REA)	Safety Engineering Management	European Railway Agency (ERA)'s method is based on European rules & regulations, with focus on risk evaluation and acceptance. Regulation details the risk assessment process for technical, operational, or organisational changes, criteria and accreditation for assessment bodies, and harmonised design targets for mutual recognition of technical systems across the EU [27].
NIST 800 series	Information & Technology Security Management	NIST has a set of guidelines, recommendations, technical specifications, and reports on cybersecurity. More specifically: NIST 800-12 gives an introduction to information security, NIST 800-37 provides a risk management framework for information systems and organizations, and NIST 800-160 provides a cyber-resilient engineering framework (CREF) [12] [10] [11].
Risk Analysis & Assessment Modelling Language (RAAML)	Common language	Object Management Group (OMG)'s RAAML specification can provide the foundation for conducting various safety and quality engineering activities including safety and reliability analysis methods. Besides the method support, linkages to the SysML model-of-interest are provided, enabling integration with and traceability to the analyses [28].
NCSC Guidance	Security Test Guidance	National Cyber Security Centre's Security Test Guidance is a white paper guiding organisations that outsource security testing of information systems. Aside from its four step framework, it provides a security-testing profile tool and compiled insights from government bodies and security firms [22].
System Profile for Effective Cyber Threat-based Risk Assessments (SPECTRA)	Common language	Object Management Group (OMG) language (under development) extends Systems Engineering languages with the means to identify the core entities and their relationships to support the task of interpreting and postprocessing a system description by automated tools and enabling cybersecurity analytics [29].

Systems Theoretic Process Analysis (STPA)	Loss-driven Systems Engineering Management	System Theoretic Process Analysis- Security (STPA) is a loss-driven Systems Engineering Management technique. It is a technique based on systems theory, with a focus on human & system behaviour and failure of controls. It applies standardized modelling languages and methods from Risk Analysis and Assessment Modelling Language (RAAML) [30].
Threat Modelling	Threat & Vulnerability Management	OWASP's threat modelling is used for capturing, organizing and analysing threats associated with a wide range of things, including software, applications, systems, networks, distributed systems, Internet of Things (IoT) devices, and business processes. The process can be integrated in a document- or model-based systems engineering approach [18].

Figure 1 below shows the type of source (standard, framework, process, method, technique, or guideline), which sources are domain or technology specific, and how they relate to the cyber-resilient design methodology of the ERP.

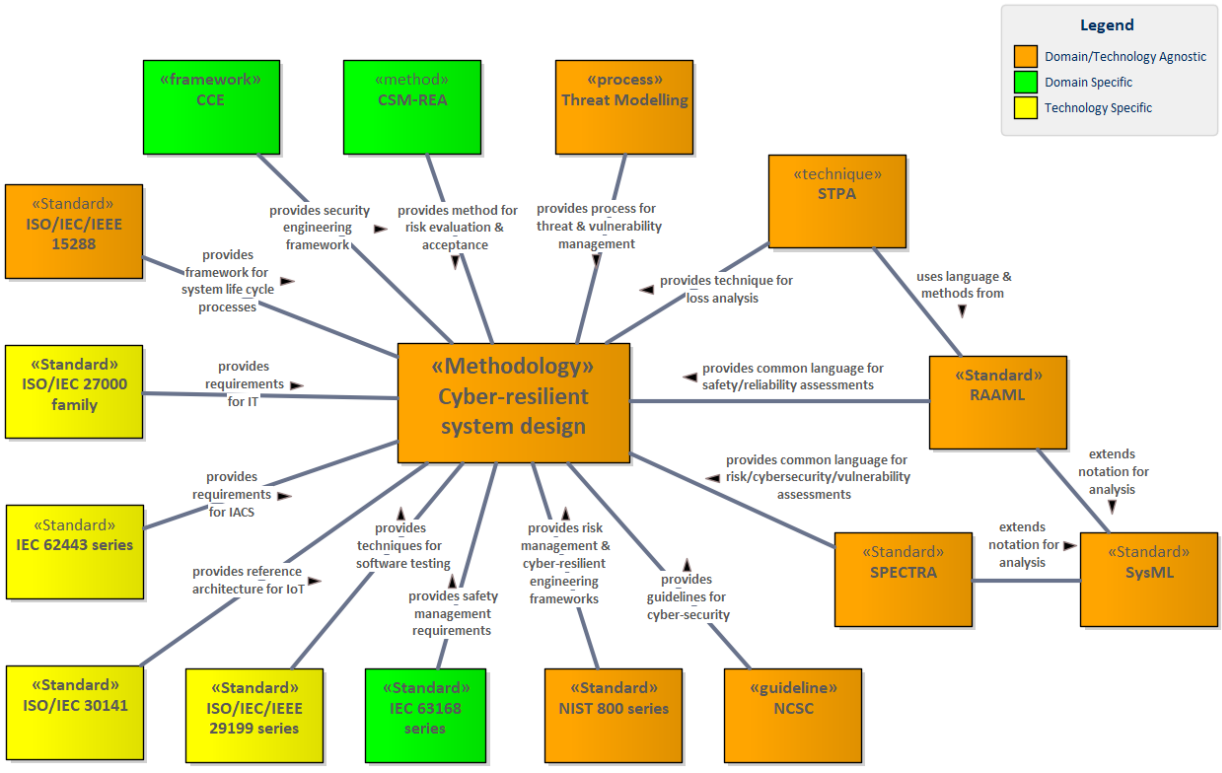

Figure 1: Domain and technology specific standards with their relationships in colour

8.3 References

[1] I.-. S. S. Board, „IEEE,” 27 March 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4578383. [Geopend 23 March 2025].

[2] I. Society, „ISO 15288 Systems and software engineering,” May 2023. [Online]. Available: https://www.iso.org/standard/81702.html. [Geopend 15 January 2025].

[3] ISO, „2700 series family,” 2025. [Online]. Available: https://www.iso.org/search.html?PROD_isoorg_en%5Bquery%5D=27000. [Geopend 5 March 2025].

[4] ISO, „IEC 30141 Standard,” August 2024. [Online]. Available: https://www.iso.org/standard/88800.html. [Geopend 19 February 2025].

[5] ISA, „ISA-62443-4-1-2018, Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements,” ISA, 1 April 2018. [Online]. Available: https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au. [Geopend April 5 2025].

[6] IEC, „IEC 63168,” March 2022. [Online]. Available: https://www.vde-verlag.de/standards/1701763/e-din-iec-63168-2-vde-0750-34-2-2022-03.html. [Geopend 15 March 2025].

[7] S. Cramer, R. Helton, R. Smith en C. St. Michel, „Idaho National Laboratory,” U.S. Department of Energy National Laboratory, June 2023. [Online]. Available: https://inl.gov/content/uploads/2023/06/Consequence-driven-Cyber-informed-Engineering.pdf. [Geopend 13 March 2025].

[8] E. R. Agency, „Guide for application of the CSM Regulation,” 1 June 2009. [Online]. Available: https://www.era.europa.eu/system/files/2022-11/Guide%20for%20the%20application%20of%20the%20Common%20Safety%20Methods%20on%20risk%20assessment%20%28EN%29.pdf?t=1751549664. [Geopend 2 April 2025].

[9] M. Nieles, K. Dempsey en V. Y. Pillitteri, „NIST 800-12- Rev 1 An Introduction to Information Security,” NIST, June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. [Geopend 2 April 2025].

[10] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau en R. McQuaid, „Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” NIST, December 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf. [Geopend 14 January 2025].

[11] W. Ross en W. Copan, „NIST 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations,” NIST, December 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [Geopend 3 March 2025].

[12] Object Management Group (OMG), „Risk Analysis and Assessment Modeling Language (RAAML) Libraries and Profiles,” December 2022. [Online]. Available: https://www.omg.org/spec/RAAML/1.0/PDF. [Geopend 22 February 2025].

[13] NCSC, „Security Testing White Paper,” Nationaal Cyber Security Centrum, 30 March 2020. [Online]. Available: https://english.ncsc.nl/binaries/ncsc-en/documenten/whitesheets/2020/march/30/security-testing-white-paper/Security+testing+White+Paper.pdf. [Geopend 12 March 2025].

[14] O. M. G. (OMG), „System Profile for Effective Cyber Threat-based Risk Asssessments (SPECTRA) version 1.0,” April 2025. [Online]. Available: https://www.omg.org/spec/SPECTRA/1.0/Beta1/Volume1/PDF. [Geopend 3 April 2025].

[15] MIT, „Introduction to STPA for Security (STPA-SEC),” April 2013. [Online]. Available: https://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/Basic_STPA_Tutorial1.pdf. [Geopend 10 February 2025].

[16] L. Conklin, „Threat Modelling Process,” OWASP, 2025. [Online]. Available: https://owasp.org/www-community/Threat_Modeling_Process. [Geopend 7 April 2025].

9 Appendix E : Application of the design methodology

9.1 Summary

The appendix provides insights from the initial application of the methodology that demonstrate its *relevance* and practical *applicability*, while also informing future developments. The insights are grouped by their source: (1) early development observations; (2) findings from expert interviews; and (3) reflections on considering an ongoing project through the methodology lens.

9.2 Introduction

In today's interconnected world, complex systems face growing cybersecurity threats. Resilience against these threats is now a critical concern. Companies have to handle more complexity and interdependencies. They need to proactively integrate of cybersecurity resilience into the early stages of systems engineering.

This appendix investigates relevance and applicability of the methodology. It outlines insights from early development steps, expert interviews, and reflections on a running project. These insights help to assess the strengths and gaps of the methodology.

The evaluation approach consisted of:

- A methodology designer's reflections on early (pre-ERP) methodology development.
- Expert interviews conducted with two experienced security architects, each interviewed individually.
- Reflections by another methodology designer on how an applied research project can be interpreted through the lens of the ERP methodology.

These components enabled to collect insights in a holistic way from different perspectives. The approach was chosen based on its practicality. It provided useful outcomes and a view on relevance and applicability of the methodology, even though the ERP Deliverable D1.1 was released only several weeks earlier.

9.3 Reflections on the early methodology development

The methodology development takes place in close collaboration with industry. Before the start of this ERP, in 2024, an initial methodology was outlined in the INTERSCT project. This methodology was demonstrated to several industry companies in the high tech industry. A few of said companies, including Vanderlande, expressed their interest in exploring relevant use cases. Vanderlande conducted a series of meetings in summer 2024 to identify system vulnerabilities and areas where the methodology can provide value.

One insight was that a complete methodology implementation may require over a year. Yet, *partial application could also yield meaningful insights*. Consequently, the company opted to focus on the risk management aspects of the methodology, which is reflected in the scope of an initiated joint TNO-ESI and Vanderlande SecureArch project. The project focused on existing system provided by Vanderlande and multiple use cases.

9.4 Insights from expert interviews

After an update of the methodology was published, we conducted interviews with Vanderlande architects to reflect on the relevant methodology steps. These discussions focused on their perspectives regarding (1) the overall methodology (Figure 4), and (2) the specific elements within the 'Safety, Security Assessment & Treatment' block (Figure 11). Both architects are actively involved in the SecureArch project. The project centres on security risk assessment, which informed the emphasis on the assessment methodology block. The architects brought deep knowledge of the company's products, development practices, and standards. Their input enabled cross-validation of observations and enriched the overall feedback. Each interview was attended by two TNO-ESI professionals to avoid interpretation bias.

9.4.1 Architects' remarks

The architects emphasized that the overall methodology (shown in Figure 4) helps highlight the importance of viewing resilience from a broad, organization-wide perspective. It is not enough if only a few internal teams focus on the topic, especially when their efforts remain isolated. They also noted that, when tailored, the methodology should be adjusted not only to specific domains but also to different countries and markets. Resilience, they argued, must be seen as more than just a list of cybersecurity requirements. A key challenge is performing risk assessments for operations when assets are used in multiple contexts. Additionally, the transfer of risks between stakeholders is a critical issue. For example, an asset owner becomes responsible for operational risks, while the capability provider must manage product risks across various use cases.

The application of the methodology facilitated the identification and exploration of several key areas for potential enhancement. In this way, exploring several clear topics helped in-depth discussions and contributed to the ongoing developments. One example is the identified need for explicit modelling of delivered solutions (to improve clarity and traceability across system components). Another concerned with the emphasis on elaborating system documentation. Moreover, the importance of strengthening feedback mechanisms within the overall systems loop were highlighted (to ensure more frequent and structured feedback for enhance resilience and responsiveness). Additionally, the methodology prompted discussions around the development of a strategic approach to risk prioritisation, enabling more targeted and effective mitigation efforts. Finally, constructing a systematic view of security controls emerged as a valuable practice, offering both operational benefits and clearer use cases for integrating cybersecurity resilience into systems engineering.

9.4.2 Architects' view on the methodology

The architects provided several reflections on the overall methodology, emphasizing its practical relevance and potential for improvement. They noted that the methodology aligns well with current practices and serves as a useful lens for identifying areas of enhancement. One

of its strengths lies in supporting the early involvement of professionals, which is considered a critical factor in shaping resilient system designs. Additionally, the methodology shows promise in linking engineering decisions to customers' business continuity and recovery plans which is an important consideration, given that many choices ultimately depend on customer preferences, such as opting for manual fallback modes. However, the architects also observed that, in its current form, the methodology offers limited direct integration with existing security development guidelines. This limitation is addressed in more detail later in the report.

The architects shared several observations regarding the 'Safety, Security Assessment & Treatment' block (Figure 20). They noted that while the elements within this block are largely complete, there remain opportunities for refinement, some of which are discussed in subsection 3.2 of this report. The block enables clear identification and discussion of topics such as the risk registry, which is considered a critical component in managing system resilience. Additionally, the methodology was seen as helpful in visualising existing processes, though attention may be needed to ensure alignment with current operational constraints, particularly in how risks are assessed in relation to the customer's business context.

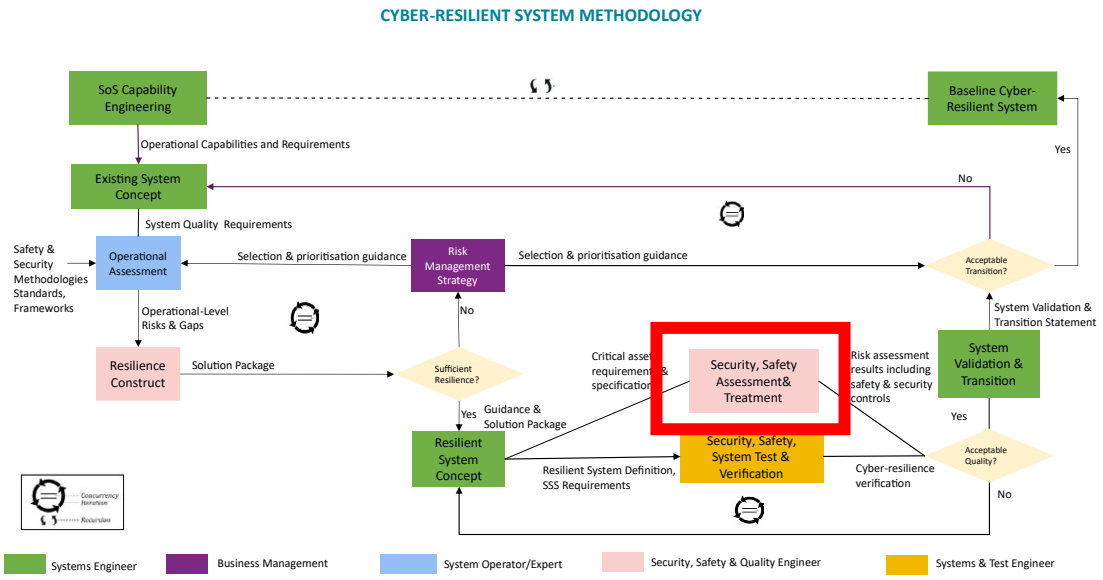

Figure 20: Meta methodology and the domain specific area marked in red.

9.4.3 Learnings from interviews

The application showed that the overall methodology is *recognisable* and *valuable for discussing current practices and improvement opportunities*. While it has limited additions to current security development guidelines, it provides an overview and assists in identifying potential improvement opportunities. To mention, the top level of the methodology was not intended to lead to direct changes in security development guidelines due to its abstraction.

It was noted that resilience is strongly determined by the customer (asset owner), who plays an important role in the process. Architecture documents (signed off by the customer) capture several boxes: Existing System, Operational Assessment, and Resilience System Concept. Moreover, resilience is multifaceted and exists on multiple layers (e.g., the number of back-up systems and individual items of hardware). Therefore, the role of the Systems Engineer

should include a clear understanding of and connections to all stakeholders, including the customers.

Company-specific processes and decision ownership may differ in relation to safety and security-related matters can be different. For instance, while safety concerns are well known and can be reused, security-related resilience might be explicitly captured in requirements and discussed with the risk owner. Tailoring of a methodology to a specific company needs to account for it.

Ways to deal with delays in system development (prior to transition) should be carefully considered. Each delay (which may last several months) makes the system more insecure. In practice, there is a need for tracking changes in relation to vulnerabilities and requirements.

The interviews also allowed us to deepen our understanding of how the block 'Safety, Security Assessment & Treatment' can be executed in practice. This informs Level 3 formulation of the methodology in the next development iteration. Insights included that risks are:

- Difficult to determine without insight into the customer's business processes;
- Capable of propagating from the customer to the high-tech company. For example, the company can be heavily impacted if more than three customers are affected.

9.5 Reflections on a project through the methodology lens

A running project can be analysed through the methodology lens to identify relevant topics and improvements. Methodology designers reflected on it as follows.

To understand how the company manages vulnerabilities and cyber-threats to existing or new designs, the team collaborated with Vanderlande. They developed a problem statement that defines the system context. This context identifies where appropriate security risk assessments and resilient measures can be applied. The goal is to balance mission continuity and cyber-resilience propositions.

The SecureArch project concentrated on assessing cybersecurity risks within system architectures. An overview of the project's actions and artifacts is presented in Figure 21, with Steps 1 through 3 corresponding to selected activities to the overall methodology. For instance, Step 1 focused on generating Data Flow Diagrams (DFDs). It serves as a preparatory activity for threat mapping and aligns with responsibilities typically assigned to the Systems Engineer role within the methodology. Step 2 corresponds to the 'Create mapping of threats' activity, while Step 3 directly supports the tasks of 'Providing risk calculation based on likelihood and vulnerabilities' and 'Calculating the security risk based on the impact on business processes.' The SecureArch project placed particular emphasis on Step 3. Both Steps 2 and 3 are closely associated with the responsibilities of the Security, Safety & Quality Engineer role as defined in the methodology.

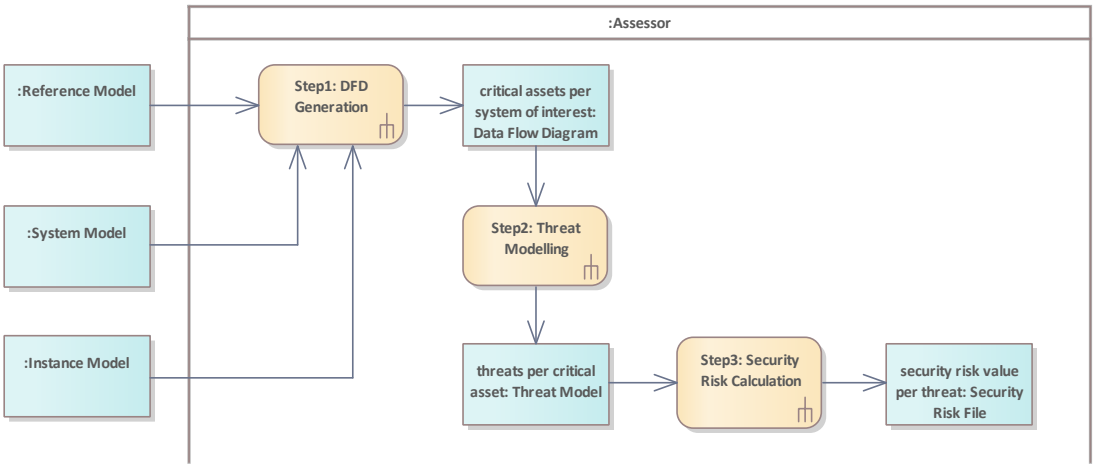

Figure 21: Security risk assessment (SecureArch project).

Risk management was approached as a system lifecycle process, extending beyond development to encompass realization, deployment, and operational use within the system-of-systems (SoS) context.

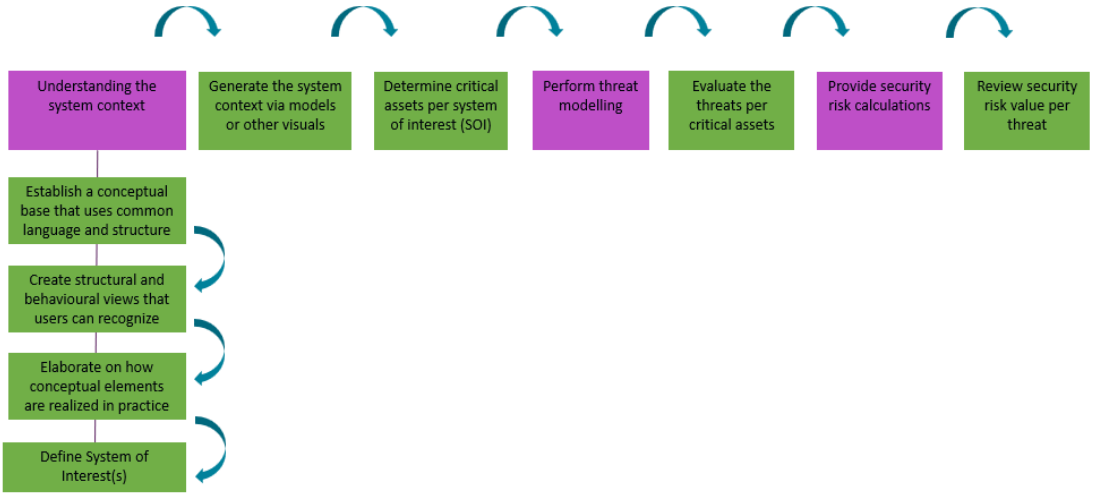

Figure 22: Security Risk Assessment Process.

Figure 22 shows the risk assessment process, where the purple boxes indicate key assessment pillars. ‘Understanding system context’ refers to recognizing critical assets and vulnerabilities present within the system of interest. ‘Performing threat modelling’ is based upon new threat intelligence during system life-cycle phases. Lastly, in ‘Providing security risk calculations’ stakeholders consider risks per threat. *This process also ensures traceability and accountability needed for resilience and business continuity.*

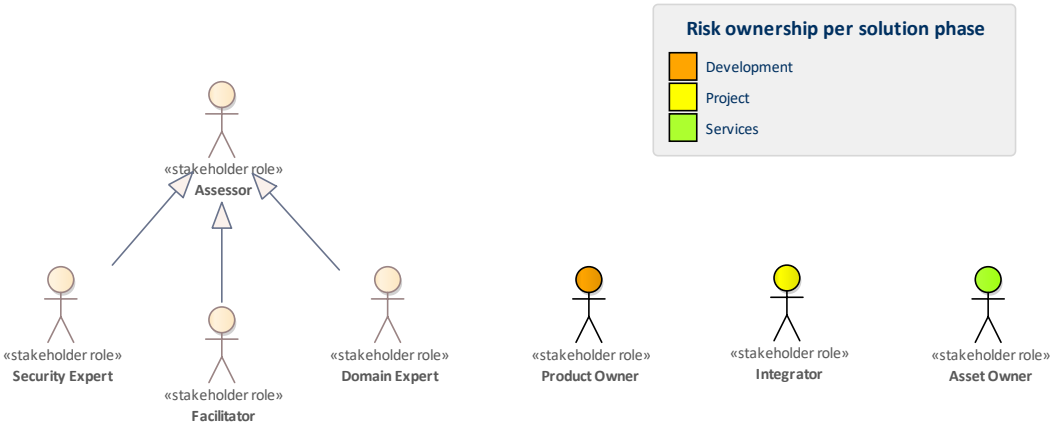

Figure 23: Actual roles with respect to risks (SecureArch project).

The team carried out interviews and workshops with Vanderlande, determined who would be the roles that would correspond to the roles defined in the methodology. The roles with respect to the specializations differed. Rather than having a systems engineer, business manager, system operator and other subject matter experts in the working environment, the team recognized that there are different roles in the organization (Figure 23) and these were due to the associated risks.

As the meta-level methodology is domain-agnostic, the team recognized there are certain differences in the methodology workflow. The team tried to apply the diagram Security, Safety Assessment & Treatment (Figure 11); however, the domain-specific method created a differentiated version from the meta-level methodology.

By itself, the SecureArch project aimed at accelerating the risk assessment process. Two key insights emerged from this effort. First, the importance of reusing assessment outputs across different phases of the system lifecycle was emphasized, enabling continuity and efficiency. Second, the project highlighted the need to distinguish risk calculations based on stakeholder roles. For example, the perceived risk for an asset owner may differ from that of a product supplier, even though they may share common interests.

Insights from the SecureArch project prompted several methodology refinements. These included clarifying the transition from system design decisions to risk management strategies and embedding the definition of security and safety controls within the resilient system concept. The project also surfaced broader challenges that can inform methodology tailoring discussions. Participants found it difficult to clearly distinguish between lifecycle phases, particularly when transferring ownership of risks or evaluating solutions with and without mitigating measures. This ambiguity highlighted the absence of a shared perspective for conducting assessments and the risk of disrupting the continuity of digital threads across the lifecycle. Mapping roles from the IEC 62443 standard proved helpful in navigating these complexities and provided a reference point for aligning responsibilities within the project.

9.6 Forward outlook

9.6.1 Potential improvements to the methodology

Based on the insights outlined above, several improvements to the methodology can be proposed.

First, *the topic of 'Identify controls & countermeasures' can be positioned outside of the block 'Security, Safety Assessment & Treatment'*. It should account for system-level trade-offs and go beyond only resilience concerns. For example, there may be a need to consult subject-matter experts (e.g., on fibreoptics) before applying countermeasures. While some suggestions (e.g., adjust filter data strategies) can be identified on a deeper level of the methodology, the decision should consider system-level impact. To mention, the latest update of the methodology already captures this identified improvement.

Second, the identification and *definition of critical assets, and selection of threats should occur prior to* discussing security risks. Otherwise, it causes difficulties to select capabilities, especially if a discussion on critical assets has not been stabilized. One example: how does one choose whether a core database or the ability for manual operation is critical?

Finally, automating the execution of the methodology is a promising area. Given the complexity of the subject (and organization capability gaps), the lack of automation may hinder methodology adoption.

9.6.2 Potential changes in domain-specific applications

Domain-specific applications of the methodology should account for a number of aspects.

- Different contexts: As some products can be used in various contexts, there is a need to explicitly address how one (sub)system can relate to multiple contexts. The specification of context(s) would play a significant role;
- Links to the customer's goals (e.g., via operational use cases or capabilities): It is specifically relevant for companies that value customer intimacy. The aspect is particularly important due to the complexities of modern value chains;
- Roles should have domain knowledge: The expertise of individual actors in the methodology need to reflect for domain-specificity and contextual understanding. For instance, certain domains, countries, and (larger) clients might have unique characteristics. To mention, the Operational Assessment block of the methodology already reflects involvement of a System Operator/Expert. The topic should also consider ways of working and methodologies of integrators. Any connection between two components should take domain-specificity into account.

9.7 Conclusions and recommendations

This appendix indicated the relevance and applicability of the ERP cybersecurity methodology to industrial practices. First, the benefits of partial application of the methodology was recognized in early stages. Then, industrial security architects suggested that the methodology assists viewing resilience from the overall perspective, avoiding siloed efforts. The main methodology flow and activities were recognized. Several improvement opportunities for industrial practices were identified by applying the methodology to discuss a running project. Also, several improvement opportunities for the methodology improvement were identified, next to focus areas for when applying the methodology to specific domains.

This initial application of the methodology offered valuable insights and directions for its further development. The feedback gathered suggests that the methodology should be updated to reflect the key aspects identified during its early use. Further validation of the revised version is also needed to ensure its relevance and effectiveness across contexts.

Industrial practitioners are encouraged to apply the methodology (in full or in part) within their projects to generate additional feedback. Moreover, the methodology would benefit from peer review by professionals in systems engineering and cybersecurity resilience. This could be achieved through peer-reviewed conference publications and collaborative research across domains in the ERP continuation.

ICT, Strategy & Policy

High Tech Campus 25
5656 AE Eindhoven
www.tno.nl

TNO innovation for life