

Security risk assessments and trade studies for
cyber-physical systems

Architecting Cyber-Physical Systems; a Multi-Objective Approach with Security as a Key Quality

TNO 2026 R10857 – 16-7-2026

Architecting Cyber-Physical Systems; a Multi-Objective Approach with Security as a Key Quality

Security risk assessments and trade studies for cyber-physical systems

Author(s)	Bas van der Leeuw, Alexandr Vasenev, Pieter Goosen
Classification report	TNO Public
Sponsor	Vanderlande
Project name	SecureArch
Project number	060.63240/01.01

All rights reserved

No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

Disclaimer

In the creation of this document, Microsoft 365 Copilot was used to improve the use of English. In all instances where Copilot was used, the authors thoroughly reviewed the results to ensure the end result is accurate and free from errors, thus allowing the authors to take responsibility for the content.

Acknowledgement

The research is carried out as part of the SecureArch program under the responsibility of TNO-ESI in cooperation with Vanderlande Industries. The research activities are co-funded by Holland High Tech | TKI HSTM via the PPP Innovation Scheme (PPP-I) for public-private partnerships.

© 2026 TNO

Contents

Summary	5
1. Introduction.....	6
Context	6
Problem statement.....	6
Company-specific (continuous) improvement opportunities.....	6
Additional opportunities	8
Research questions	8
Outline of the report	9
Document history.....	9
2. Security Architecting	10
State of the art and state of practice	10
State of the art	10
State of practice.....	10
Methodology Description.....	11
Processes	12
Artefacts	13
Stakeholder Roles	15
Activities	16
Method Evaluation	17
Evaluation approach.....	18
Selection of a use case	18
Preparing the workshops.....	19
Executing the workshops	19
Observations and discussion	19
3. Conclusions and Future Work.....	21
Conclusions	21
Future Work	24
Reusable Assets	25
4. Bibliography	26
Glossary	28
Appendices.....	30
State of Practice investigation for trade-off analysis.....	30

Summary

This report shares the learnings of TNO-ESI and Vanderlande on architecting cyber-physical systems. It is the final result of the SecureArch project.

The purpose of architecting is to generate system architecture alternatives, and select the most effective one(s), for guiding the design process in defining a solution that can be realised. Due to the interconnectedness of cyber-physical systems, security has become a key quality that must be considered in the selection process.

The effectiveness of alternatives depends on (multiple) business goals and operational capabilities. The SecureArch project focused on automated parcel handling solutions. After performing a problem analysis with Vanderlande for this application domain, the overall problem statement was identified as follows: *"How to create & evaluate alternative concepts and manage architectural design decisions, risks, and measures effectively, balancing security and other quality attributes?"*

Applied research was done on a methodology for creating and selecting alternatives (architectural trade-offs), and performing security risk assessments. The risk assessment approach was evaluated for two cases, involving multiple stakeholders in workshops. The absence of a clear use case for a trade-off study prevented the validation of the complete methodology.

Nevertheless, the methodology described is considered to be promising when dealing with uncertainty and need for a balance between multiple competing objectives. Key to the approach would be to ensure that:

- The objectives under consideration as selection criteria for alternatives, should be the same as the ones used for risk assessments;
- The objectives should be measurable, so dependencies between them become clear and allow for reasoning about competing and enforcing objectives;
- To save time and resources, (security) risk assessments should be applied to selected alternatives only.

To save communication time, increase efficiency and manage consistency and complexity it is recommended to further research a model-based approach, which will save time, resources, and ensures the completeness, promptness and accurateness of the trade-off. However, this capability will require appropriate competencies of the people involved and support from the organisation (processes, tooling, training, etc).

1. Introduction

Context

Cyber-physical systems (CPS) are still an emerging topic with no precise and universal agreed definition [1]. Key CPS characteristics are the interconnectedness with the internet and its users, and tightly coupled physical and software components (computing controls physical processes). This differs from "traditional" industrial automation and control systems (IACS), which often assumes the use of isolated networks and proprietary communication protocols (that some consider as being sufficient for protection). However, this assumption is unjustified, as since the Stuxnet attack, numerous subsequent attacks on IACS have occurred [15].

The interconnected nature of CPS brings significant security concerns. CPS must address not only safety and availability but also security, and integrity. Furthermore, security for CPS has become a legal and regulatory requirement. Relevant legislation originates from various regions. For example, in the United States, the "Postal and Shipping" sector is considered part of critical infrastructure [16]. The EU has introduced several other relevant directives and regulations [17, 18, 19, 20, 21]. China formulated laws for cybersecurity, data security and personal information protection for Southeast Asia [22]. This generic overview illustrates the global context for the parcel domain and mandatory requirements CPS have to comply with regarding security and safety.

The vision and outlook for Systems Architecting and Systems Engineering in the high-tech equipment industry [23] mentions Digital Engineering and MBSE as key enabler for improving effectiveness and efficiency. In this project, applied research was done on improving the effectiveness and efficiency of Systems Architecting with security as a key quality.

Problem statement

In addition to compliance requirements, the rapid evolution of CPS and their advancing technologies, such as: artificial intelligence (AI), internet of things (IoT), machine learning, and cloud computing; makes dealing with vulnerabilities to cyber threats a key concern [2].

The Dutch high-tech manufacturing industry requires a suitable methodology to address a continuously changing threat landscape. The traditional 'incident-driven approach' that is applied to manage safety risks needs to become more agile, anticipating a changing CPS environment for managing security risks. Appropriate security risk assessments and careful considerations of trade-offs are essential to ensure balanced solutions with acceptable quality.

The SecureArch project was organized in two phases. The first phase examined security risk assessment. The second phase focused on architectural trade-offs, involving interrelated quality attributes affected by security. These approaches were applied to Vanderlande's use cases and offerings. Both phases are covered in this report.

Company-specific (continuous) improvement opportunities

During the project, company experts were interviewed that led to the identification of opportunities for further enhancing processes and communications:

1. Decision management and Risk management processes, considered as typical Systems & Software Engineering Lifecycle processes [3], could be enhanced by integrating security considerations. Additionally, System analysis and Measurement processes could add value to performing trade-offs (in particular, towards a shared understanding and reuse of analytical models for balancing system architecture alternatives and integrations with 3rd party equipment).
2. There is an opportunity to clarify how trade-offs between security and other system qualities are managed. By further considering security alongside reliability, costs, and integration with the customer's system, the company can enhance its approach. Additionally, a clearer understanding and communication of the organization's risk appetite (and the customers' risk appetites, which may differ significantly across customers) will support even more informed decision-making.
3. The company's reliance on informal methods can be further enhanced with developing shared security

perspectives and formalized processes. By strengthening governance, ownership, and management of security risks and decisions, the organization can further advance its security posture and foster continuous improvement.

Figure 1 summarizes key findings from the interviews as interconnected Drivers, Challenges, and Opportunities. The arrows in the figure indicate dependencies (e.g., a 'Challenge' depends on a 'Driver').



Figure 1: Key Drivers, Challenges, and Opportunities

The key drivers originate from external regulatory requirements, customer expectations, and supplier responsibilities. Challenges mainly arise due to shifts in business models, such as the evolution from project-based delivery to product-oriented approaches and the transition from engineering-to-order to configure-to-order processes.

Illustrative (and not exhaustive) list of examples include:

- Drivers: External regulations shape requirements and expectations. For instance, NIS2 [18] requires greater transparency regarding incident disclosure and customers increasingly expect visible process maturity, The CRA [20] mandates delivery of timely software updates. EU Machinery Regulation [21] requires the inclusion of cybersecurity in the machinery risk assessment and protection against intentional interference;
- Challenges: Some gaps in application domain knowledge can be further addressed. One example is a shared understanding of cybersecurity principles across stakeholders (especially as customers worldwide are governed by different legislation and have diverse maturity levels and security requirements);
- Opportunities: Adopting more structured trade-off methodologies by using standardized approaches. It includes considering how to handle trade-offs studies and define relevant roles. This will assist in improving security awareness and knowledge, as well as establishing a system-wide structured security approach. The use of models can help automate risk assessment and trade-studies through reuse and feedback.

Importantly, regulations and standards require security by design, meaning that security risks must be

systematically addressed from the earliest design stages and throughout the a system's lifecycle, rather than added later as compensating controls. This process starts with sound architectural design decisions.

The project considered the identified opportunities in relation to the project timeline to further refine its focus. Several important elements were recognized (e.g., 'alternative concepts' in relation to 'trade-offs', and 'managing decisions' based on the 'Company-specific Decision management and Risk management processes').

The overall problem statement was formulated as follows:

How to create & evaluate alternative concepts and manage architectural design decisions, risks, and measures effectively, balancing security and other quality attributes?

Additional opportunities

This problem statement mentioned above was identified through qualitative interviews within the organization, focusing on prevailing operational practices. Alternative solutions are available to address the issue. Implementing revisions to established workflows can provide organizational benefits.

Security requires management of information on risks, decisions, and measurements through the lifecycle. The current approach to security risk assessments and trade-off practices within the company, as well as in comparable organisations, relies predominantly on document-based processes. This presents additional challenges in efficiency and resource utilisation, particularly under time constraints and complex integration scenarios. This may lead to issues related to managing information. Moreover, considering security solely as a loss-driven quality (rather than an opportunity) can result in it being treated merely as a qualifying requirement rather than as part of the holistic trade-off analysis, especially in environments customers see security as a differentiator.

Carrying out trade-offs in a model-based systems engineering environment can offer several advantages. For instance, ISO 15288 [3] mentions that "through data query and analyses, modelling allows comparison of solution alternatives much more expeditiously, comprehensively, and accurately than can be executed through manual review of data. Solution alternatives can be compared by query and analyses against a common set of requirements functions, and key performance parameters". This is particularly relevant for security, as risk management must be revisited frequently throughout the lifecycle (e.g., whenever vulnerabilities are discovered, security updates are implemented, or a software release introduces new features).

Research questions

The original research question from the SecureArch project plan was defined as follows:

How to architect for a continuous, adaptive cyber-risk management approach for the complete lifetime of the system, in balance with value-oriented system qualities to sustain customer value and operational continuity?

As this original question is rather broad, it was refined by a problem analysis for both project phases 1 and 2, resulting in the problem statement as mentioned in the former paragraph. Figure 2 illustrates the breakdown of the original question towards more specific questions that address the problem statement. The project research objective is to answer these questions.

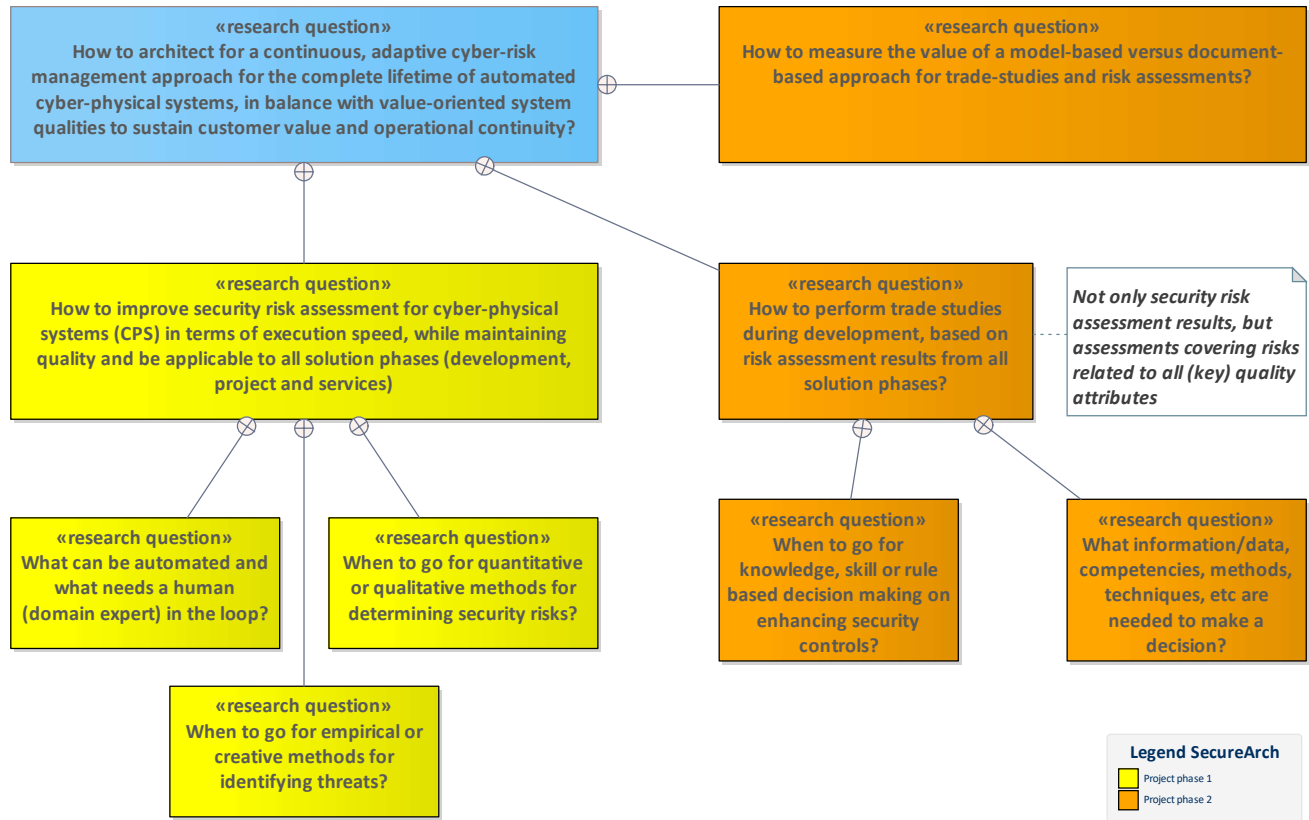


Figure 2: SecureArch research questions

Outline of the report

Chapter 1 introduced the context, problem statement, and research questions.

Chapter 2 explains the state of the art and state of practice, describes the methodology, and summarizes method evaluation.

Chapter 3 presents conclusions and recommendations for future work.

Document history

Version	Scope	Purpose for change
Initial Report	Learnings phase 1	Work product
Intermediate Report 1	Learnings phase 1	TNO-ESI peer review processed
Intermediate Report 2	Learnings phase 1 and objectives phase 2	Industry Partner review processed. Problem analysis updated for phase 2.
Concept Report	Learnings phase 1 & 2	TNO-ESI peer review and confidentiality check by Industry partner
Final Report	Learnings phase 1 & 2	TNO-ESI quality review for publication
Released Report	Learnings phase 1 & 2	Upload to TNO Digital Library for publication

2. Security Architecting

Architecting focuses on guiding design decisions under uncertainty and competing objectives, whereas design is primarily driven by system requirements. For complex systems, a system architecture is essential in transforming stakeholder needs and requirements towards 'the right' system requirements, and tracing system definitions towards concept definitions.

As CPS grow in complexity, adopting a structured multi-objective decision making approach becomes essential. Risk assessments are critical to this process, ensuring that uncertainties and potential impacts are understood and managed effectively. Together, trade-off studies and risk assessments are fundamental for resilient decisions in complex environments.

It is important to understand that security as a quality needs to be balanced with other qualities. It cannot be considered in a silo and needs to be part of the system architecting & design activities - it cannot be bolted on afterwards.

State of the art and state of practice

For architecting and selecting alternatives that best balance conflicting objectives, different approaches can be taken. In this project, the state of the art and state of practice was investigated to align innovations for the Dutch high-tech manufacturing industry with their current capabilities, avoid reinventing the wheel, and identify research gaps.

The general state of the art and more specific state of practice for the Dutch high-tech manufacturing is described next.

State of the art

Within the International Community of Systems Engineering, model-based approaches are emerging [25, 26], and data driven decision making is considered to be the state of the art for complex systems. The Multi-Objective Decision Approach (MODA) is considered to be best practice according to the global Systems Engineering community [10]. The Software Engineering domain considers the Architecture Tradeoff Analysis Method (ATAM) as the leading method [24]. The distinction between ATAM and MODA is mainly one of decision scope. ATAM is focused on evaluating a given software architecture, and MODA on a quantitative comparison of competing system architecture alternatives against multiple stakeholder objectives.

Both approaches are complementary with traditional risk analysis methods, such as: fault tree analysis (FTA), failure modes and effects criticality analysis (FMECA), event tree analysis (ETA), and hazard operability analysis (HAZOP). In addition, Systems-Theoretic Process Analysis (STPA), which extends traditional safety analysis methods by focusing on unsafe control actions and system level interactions, is particularly useful for CPS where safety, security, and operational resilience are tightly coupled. Highly regulated application domains like medical, aerospace, automotive, and railway transportation, are typically more familiar and mature in using these methods.

Combining MODA with a model-based approach for trading off alternative concept definitions still has a gap in applied research. ISO 15288 [3] identifies the earlier mentioned benefit for MBSE in the ability to perform trade-offs, however this has not been validated for the Dutch high-tech manufacturing industry.

Research on successfully integrating early V&V in industrial MBSE [11], shows there is limited scientific proof available because it is highly dependent on "7 success factors". These success factors often are a challenge to facilitate or combine in a single project, so a more programmatic approach is needed to define and realize valuable transitions for a specific domain, enterprise, or eco-system.

State of practice

This state of practice represents the findings of 3 semi structured interviews that were conducted with architects in 2 companies in the high tech equipment industry that are ESI partners. No interviews were held with partners from the (highly regulated) medical domain. More details can be found in [Annex 1].

Trade-off analysis is primarily conducted cognitively and captured in documents. Architects and specialists

reach decisions through discussion supported by targeted analyses, with limited use of formal methods.

Early-phase assessments rely heavily on intuition and experience. To control cognitive load, complexity—particularly relationships between factors—is minimized. Conflicting objectives are typically addressed in isolation, and security is not seen as an opportunity for meeting objectives but as a compliance risk that must be met. By leaving security outside the trade-off scope, alternatives are not balanced taking into account the value security might bring in relation to other qualities, where security in itself already consists of competing objectives (like confidentiality, integrity and availability).

A variety of tools are used, including decision matrices, informal “menu card” comparisons, and discipline-specific analytical models. Trade studies involve multiple stakeholders, including business and market representatives.

No automated or model-based decision frameworks are applied, and concepts, evaluations, and rationales are seldom reused. This limits knowledge retention across development stages.

The interviews indicate that engineering productivity could be improved through more systematic decision and knowledge management processes.

Methodology Description

The methodology described in this paragraph suggests a set of related processes, methods, techniques and tools to create and evaluate alternative concepts, and manage architectural design decisions, risks, and measurements in the system lifecycle.

The methodology is built on the life cycle processes of ISO 15288 [3]. In phase 1, we focused on the assessment process, which uses artefacts produced by the architecture definition process and produces artifacts that feed risk management. In phase 2 of the project, the scope of the methodology was expanded by including the system analysis, measurement and decision management processes.

Opportunities for a model-based methodology were explored. For the SecureArch project, we scoped "the 7 success factors" [11] as followed:

1. Realistic problems: focus on industrial automation for parcel distribution in the context of transportation services, and providing services like health monitoring and patching (often by request of the customer);
2. Standardized use case: focus on alternative creation, selection and assessing security risks for the selected alternatives
3. Integration with existing tools: use existing and familiar tools that implement both SysML and threat modelling (in the project we used Sparx Enterprise Architect, since both project partners have experience in using the tool)
4. Low effort from users: modelling support by experts from both partner organisations
5. Blended/flexible modelling: linking threat models to architecture models
6. Industrial standard alignment: linking systems engineering to industrial automation, security, and safety standards [3, 8, 20, 21]
7. Modelling supports several needs: focus on the need for architectural design decisions

There is a strong relation identified with the Exploratory Research Programme (ERP) on cyber-secure systems by design [4]. Experiments from this project will be used for validation purposes of the ERP. To summarise: SecureArch dives deep into architecting, whereas the ERP focuses on design.

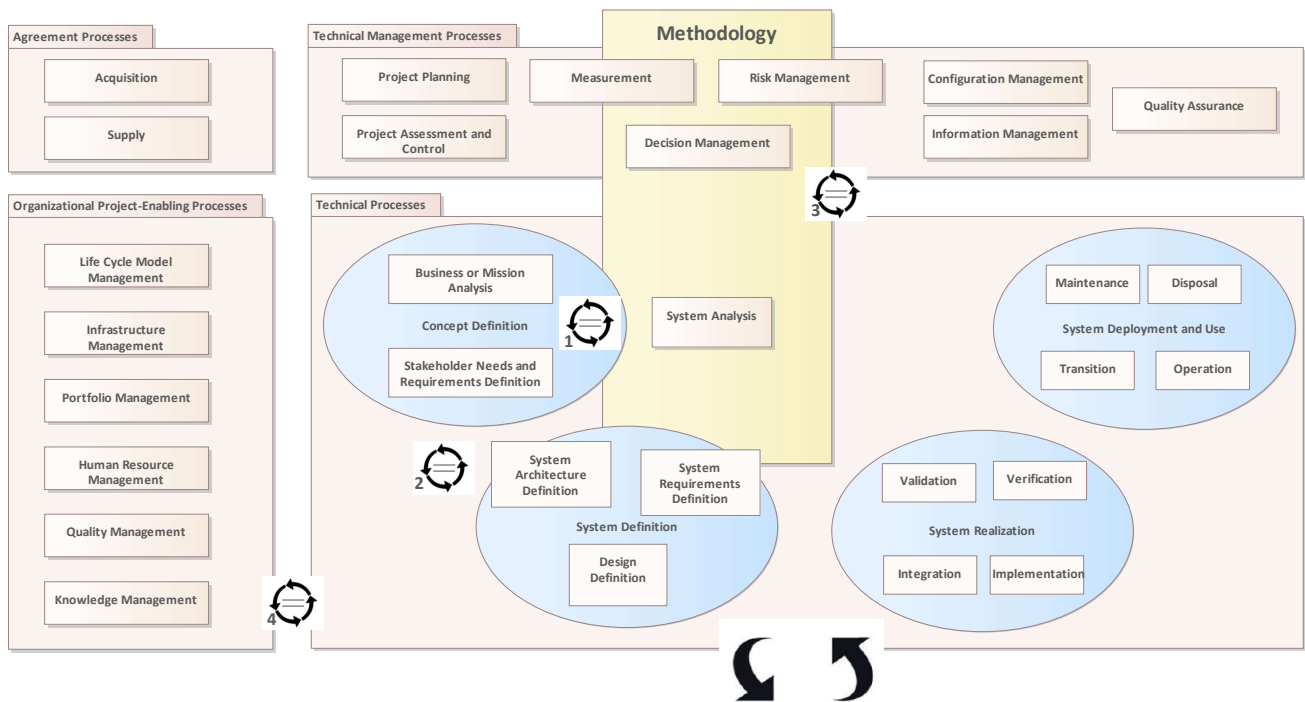


Figure 3: ISO 15288 Life Cycle Processes

Figure 3 illustrates four relevant iterations:

1. Between business analysis and stakeholder needs and requirements definition. Connecting the business and application to the technology and solutions. Often a system of interest will be part of multiple solution contexts (customer environments or even application domains), which may lead to multiple objectives that should be balanced and measurable in terms of effectiveness (MoE)
2. Between concept and system definition. Technology should be fit for purpose and feasible to be implemented with appropriate key performance parameters (KPP)
3. Between technical management and technical processes. Risks, measurements and decisions should be integrated in a technical management approach for the entire lifecycle of both products and solutions;
4. Between organizational (project-enabling processes) and technical processes. Reusable knowledge assets for projects or products, like multi-objective functions and risk matrices should be managed at organizational or domain level and not per project or technical discipline.

The purpose of the methodology is to select system architecture alternatives by assessing MoE's and KPP's, rather than continuously improving performance without a clear need. The system architecture definition process creates alternatives for a concept definition, and transforms business goals & stakeholder needs towards system requirements that drive design.

Processes

A process is generally defined as a purposeful set of activities that produce or consume artifacts, having a stakeholder role responsible for one or more of these activities. This definition along with a best practice for process modelling [5], is an extension of the ontology used for building competency models, which was explored in the ArchSkills project [6]. Figure 4 illustrates the (partial) ontology for process modelling.

Note: This ontology can be extended to full RASCI relations between Stakeholder Role and Activity, and it should be kept in mind that a Stakeholder Role can be played by one or more Person or an Enterprise.

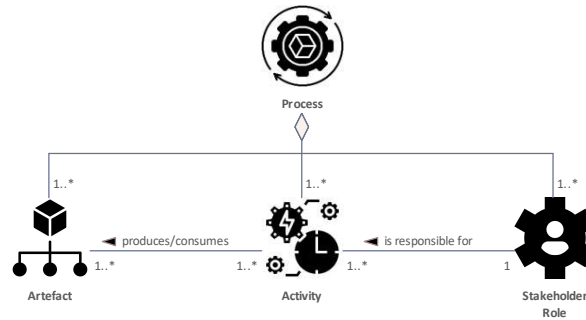


Figure 4: Process Ontology

There are many good process descriptions available for doing trade studies (like the one provided by MITRE [12]), and security risk assessments (like the one provided by OWASP [13]). The issue with these approaches is that security is considered in a silo. To solve the problem statement and be able to balance multiple objectives, the MODA approach was selected as a reference [10].

The Decision Management Process as part of MODA consists of ten activities that produce/consume artefacts to/from the other Systems Engineering Processes in iterations during the lifecycle. These activities are:

1. Frame Decision
2. Develop Objectives & Measures
3. Generate Creative Alternatives
4. Assess Alternatives via Deterministic Analysis
5. Synthesize Results
6. Identify Uncertainty & Conduct Probabilistic Analysis
7. Assess Impact of Uncertainty
8. Improve Alternatives
9. Communicate Tradeoffs
10. Present Recommendation & Implementation Plan

In the project the approach was simplified by identifying two key processes as part of the methodology:

1. Prepare & perform trade study; covering the first five activities of MODA. The purpose of this process is to generate and select the most effective system architecture alternative(s) that fit both business goals and stakeholder needs as part of the concept definition;
2. Perform (security) risk assessment; that considers the uncertainty (risks or opportunities) for potential system architecture alternative(s) and updates (security) risk files for both the system of interest (product) and solution contexts (applications).

Creating and selecting alternatives typically is done early in the lifecycle of a system (concept definition) with a high level of uncertainty, whereas security risk assessments can be done anywhere in the lifecycle, when uncertainty may be reduced and more detailed design information is provided on critical assets, vulnerabilities, and threats that may lead to an updated security risk profile. Assessing and balancing security objectives against other qualities (like: availability or safety), requires knowledge on both technology and application domain.

Note: processing the trade study and risk assessment results, which is also covered by MODA (it refers to activities 8, 9, and 10) is left out of scope for this methodology. It is seen as part of basic technical and management process activities and requires no further research at this time. A large part of these activities can be automated and therefore is in favor of a model-based approach.

Artefacts

The figure below shows the artefacts that are produced by the methodology. In color coding, it is also clarified how these artefacts are related to inputs/outputs from/to technical, management, and organizational processes.

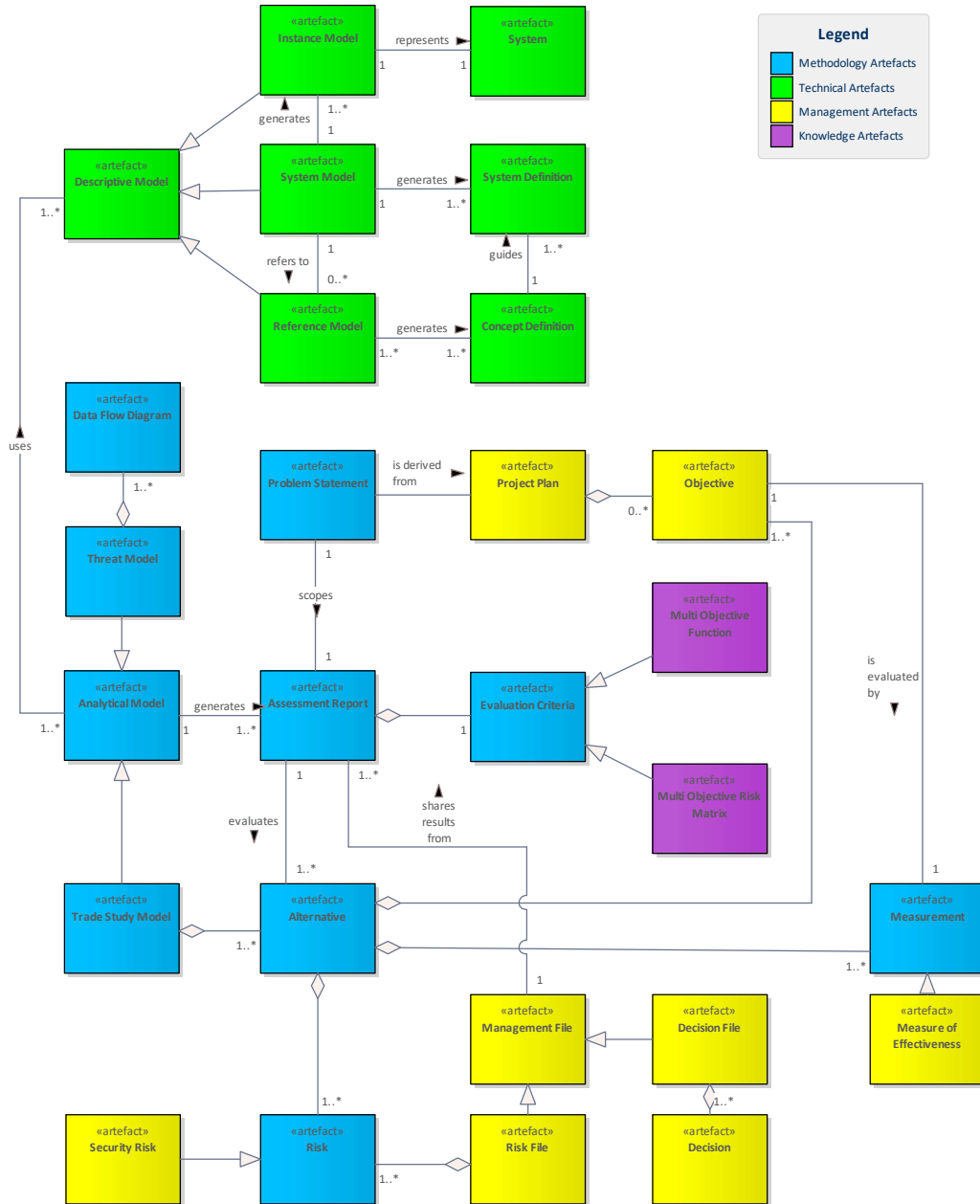


Figure 5: Methodology Artefacts

When using a model-based approach, architecture descriptions can be generated by descriptive models. Typically, a system model may refer to one or more reusable reference models. Instance models that represent the real system in the field can be generated from a system model.

Descriptive models are used by analytical models. Two examples of analytical models are a discipline specific threat model for security risk assessments and a system level trade study model for selecting system architecture alternatives.

From these analytical models assessment reports can be generated that evaluate security risks for potential alternatives or evaluates creative alternatives in terms of effectiveness towards multiple objectives, respectively. Evaluation criteria to support the assessment can be formalized at an organizational level by a multi-objective risk matrix or function.

To ensure assessment results are shared across the system lifecycle, management files can be updated and transferred across project phases from development towards realization, deployment and use. Examples of such management files are risk or decision files, providing the rationale for selecting a system architecture alternative.

Stakeholder Roles

In this project, we consider the role of a Business Owner that is both Product Supplier and Service Provider and deals with a transition from original equipment manufacturer towards original design manufacturer, and providing value added services like integration services (including third party equipment) and security updates for sustaining operational solutions. Another type of Business Owner is the Asset Owner, or the customer that acquires products and services from Product Suppliers and Service Providers.

The figure below shows the involved stakeholder roles, in which distinction is made between enterprise and person/group roles. The overview also contains a mapping towards the "Systems Engineering Roles for a New Era" [9], so it can be more easily mapped to the INCOSE SE competency framework [14].

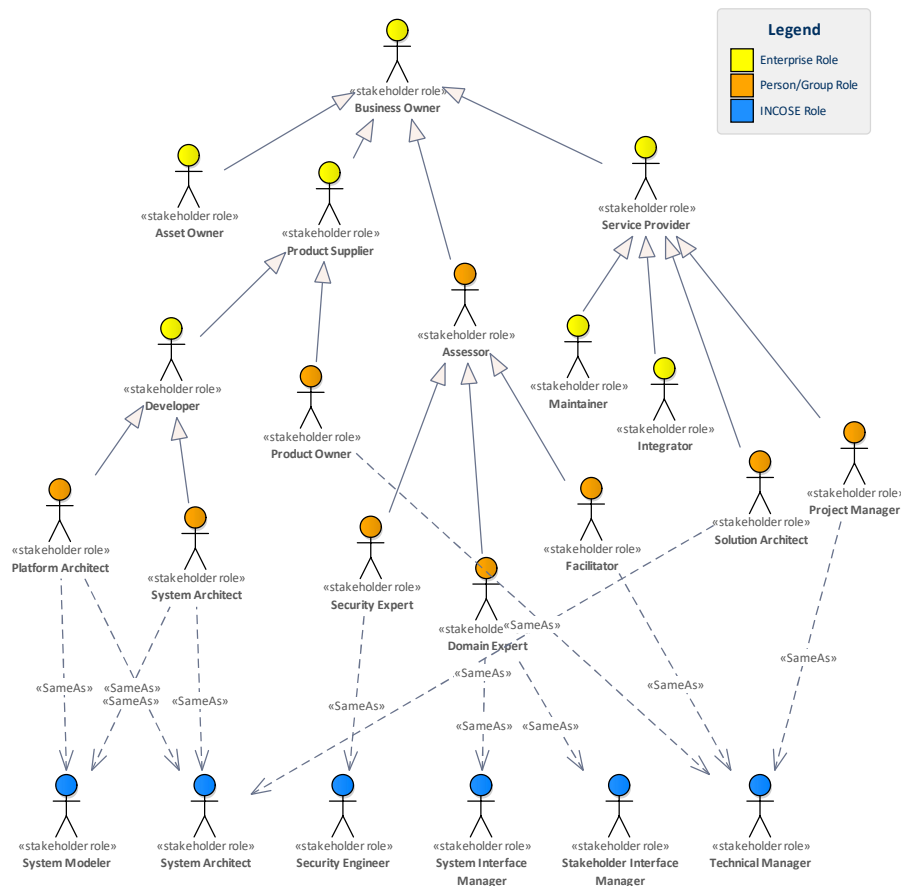


Figure 6: Methodology Stakeholder Roles

Security risk assessments consist of activities that require multiple roles. It requires domain expertise of both application (stakeholder interface manager) and technology (system interface manager), and it requires security expertise.

Depending on where you are in the lifecycle, different risk owners were identified. During development, the Product Owner should own risks for his product and its use cases; which should also cover for the product's intended use within multiple solution contexts. During project execution, the Project or Integration Manager is considered to be the risk owner for a specific solution. Ownership of remaining risks should be transferred towards the Asset Owner when the solution is deployed and put into service.

Trade-studies for selecting system architecture alternatives are needed early in the lifecycle, when a concept needs to be selected for a customized solution by the solution architect or a standardized product as part of the product portfolio or platform (system or platform architect). In a model-based approach, the system modeler might become a new role delegated by the relevant architect for building descriptive and/or analytical models.

Activities

Combining the artifacts and stakeholders with the activities in a process behaviour view, results in the two diagrams below. Figure 7 shows the activities related to preparing and performing a trade-study, and Figure 8 illustrates the security risk assessment activities. According to MODA, a trade-study precedes a risk assessment, so only risks associated with potential alternatives are assessed. This saves assessment time and resources. Both processes are subject to the iterations shown in Figure 3.

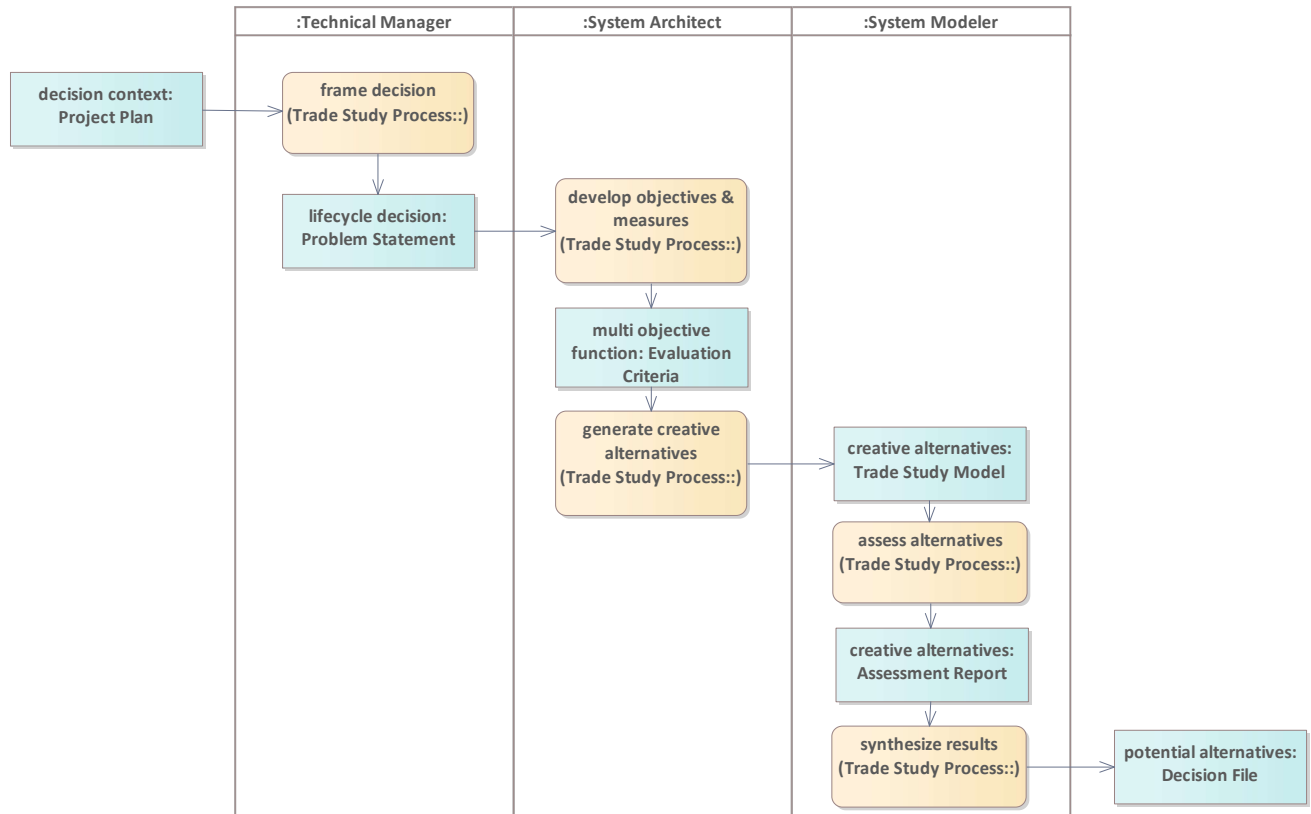


Figure 7: Prepare & Perform Trade Study

The process of preparing and performing a trade-study consists of 5 activities:

1. frame a decision: based on the objectives from the project plan, identify the decision maker (including others that should be involved), system of interest, lifecycle phase and milestone/tollgate to pass
2. develop objectives and measures: make the objectives from the project plan smart enough (at least having measures of effectiveness), so a decision can be made with the right level of accuracy needed to pass a milestone/tollgate
3. generate creative alternatives: define alternative concepts for a system of interest and determine its measurement values (based on expert or documented knowledge)
4. assess alternatives: compare alternative concepts based on a multi-objective function
5. synthesize results: curate the outcome of the assessment to highlight pro's and con's

MODA as a method is considered 'state of the art' for the high-tech industry. Due to lack of a realistic use case, we were not able to validate the method properly. In a demo it was shown that when combining MODA with parametric modelling, the steps of performing a trade-study can be automated. Developing a proper multi-objective function suitable for both application domain and technology is key.

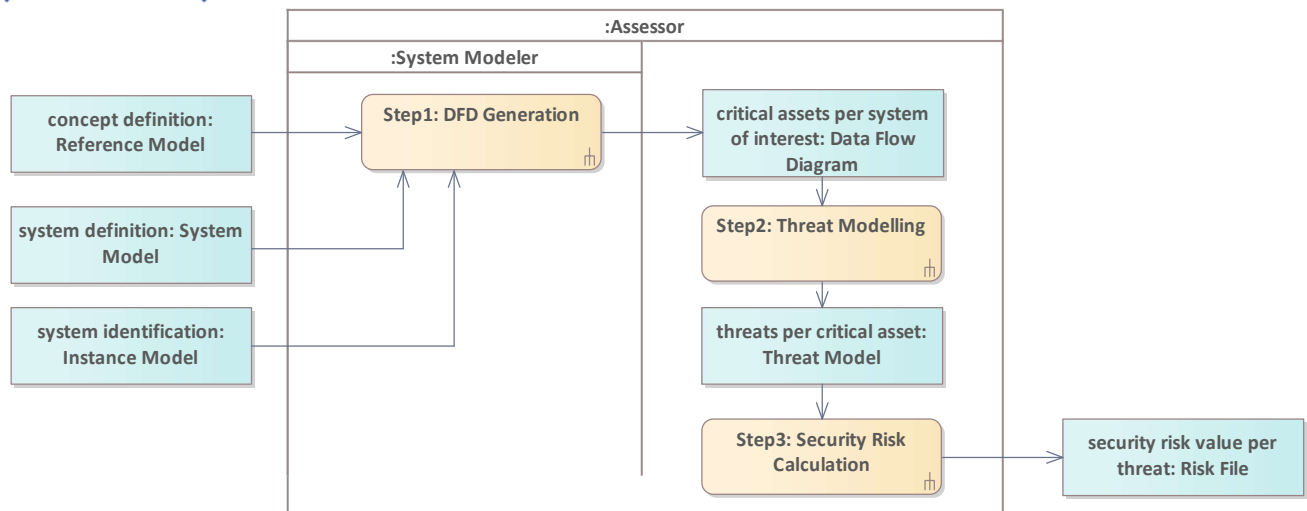


Figure 8: Security Risk Assessment

Three steps are identified for:

1. Transforming architecture descriptions towards the critical assets (logical/physical process within a specific trust boundary) and vulnerabilities of a system of interest that may need protection;
2. Identifying and updating the threats per critical asset, based on new threat intelligence that becomes available during development, project or services phases;
3. Calculating the security risk value per threat, which in the end will be treated by the stakeholder owning the security risk associated with the system of interest.

Using Data Flow Diagrams (DFD's) and Threat Modeling as a method is not new and can be considered 'state of practice' for the high-tech industry. Therefore, in phase 1 of the project, we specifically looked in more detail towards methods for calculating security risks. However, a model-based approach for the DFD generation and threat modelling steps was applied for validation purposes. The method of using a multi-objective risk matrix for calculating security risks is further explained and evaluated in the next paragraph.

Risks associated with potential alternatives should be measurable against the same objectives as developed in the trade-study. Treatment of risks should be done holistically, considering security in relation to other qualities. In general, there are four approaches to treat a risk [7]:

1. Acceptance: Accept the risk and do no more;
 2. Avoidance: Avoid the risk by change of requirements or redesign;
 3. Control (or Mitigation): Take actions to reduce likelihood and/or impact over time;
 4. Transference: transfer the risk by agreement with another stakeholder (for example a service provider)
- Potential alternatives can be converted (optionally via another trade-off) towards the most feasible system architecture definition that guides design.

Method Evaluation

This section reports on evaluating the method for security risk calculations based on two practical use cases. It contributes to answering the research question 'What information/data, competencies, methods, techniques, etc are needed to make a decision?' In particular, the findings below emphasise the importance of preparation activities and the roles, including their desired involvement.

We focused on how to organize and speed up group estimations of risk likelihood and impact. Such an assessment can be carried out in different phases of the lifecycle. We specifically focused on an initial assessment in the process, when previous assessments are unavailable as reference points. Subsequent assessments can then focus on differences with the initial one, saving time and resources.

We selected workshops as a technique and in total we: prepared, conducted, observed, and analyzed three workshops.

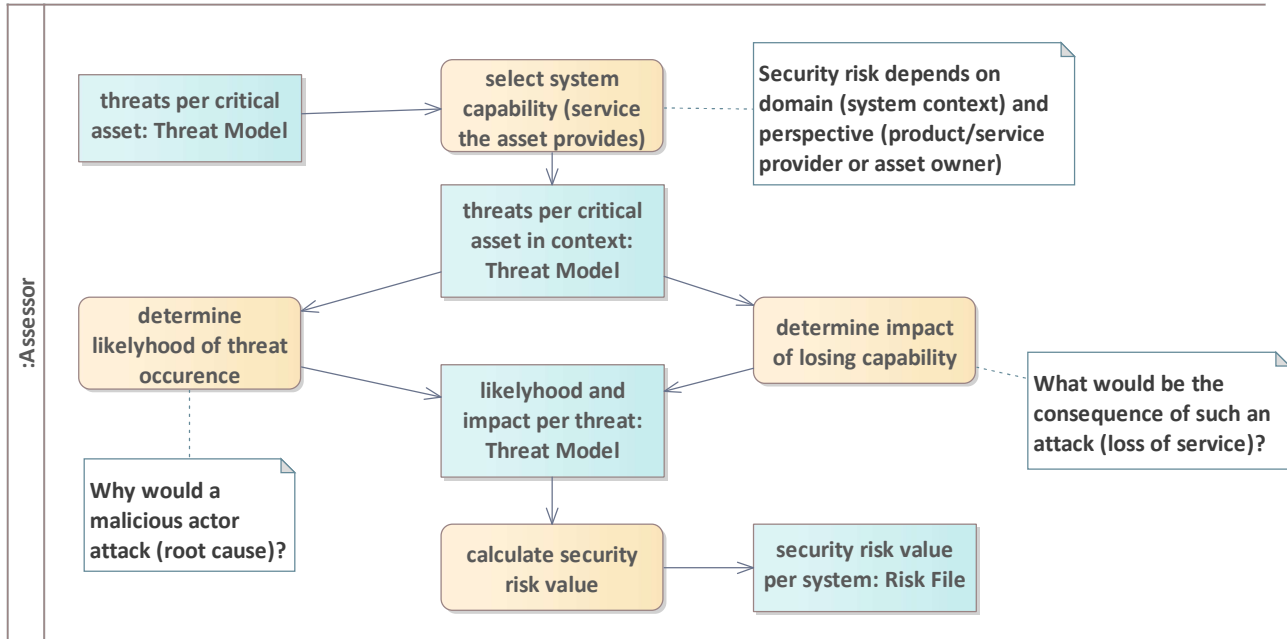


Figure 9: Security Risk Calculation

Figure 9 illustrates in more detail the steps for calculating a security risk:

1. The first step is to ensure there is a shared understanding of the product and services provided.
2. Once this context is clear, the likelihood of a threat occurrence and impact (such as financial, operational, and environmental effects on both customer and supplier) can be determined.
3. Finally, the risk value can be calculated using a heatmap or 5x5 risk matrix as artefact provided by the (corporate) risk management process. Heatmaps or 5x5 risk matrices are well known artefacts within the Risk Management domain, showing (typically 5) classifications for both probability and impact as criteria for: acceptable, tolerable, and unacceptable risks.

Evaluation approach

To ensure a comprehensive evaluation of the method for calculating security risks, we conducted the following steps:

1. Select a use case;
2. Prepare for execution of method;
3. Execute the method on selected use case;
4. Share observations on preparation and execution and consolidate findings.

Selection of a use case

To choose a case we constructed the following criteria:

- Need to address key research questions and relevant to identified challenges;
- Address a real pain for involved stakeholders (problem owners);
- Feasible in terms of available resources and information / data;
- Additional (nice-to-have) criteria: relevance to a follow-up research and other lifecycle stages; relevance to other (public) TNO research project.

The industry partner proposed 4 potential use cases. After ranking them on the scale from 1 to 10 against the main criteria, the project selected:

1. Digital Readiness: considering remote data collection and transfer for predictive maintenance. It connects on-premise and cloud services with broad security challenges.
2. Safety Instrumented System: concerning safety critical control functions with remote monitoring services. It relates security to safety risk assessments.

The first case was covered in two workshops. The first workshop introduced the case to the participants who discussed threats. The second workshop focused on assessing risks. A third workshop was spent on the second case. Workshops were prepared as follows.

Preparing the workshops

Based on architecture descriptions and interviews with architects we created Data Flow Diagrams and identified a list of threats for the case. The diagrams were created in Sparx Enterprise Architect.

We specified the assessment roles as described in Figure 6 and allocated them to the workshop participants. Attendees from TNO-ESI acted as observer and assisted in facilitation.

To enable risk calculation prior to or during the workshop an Excel template was constructed for workshop participants:

- With description of individual threats (from DFD with some context);
- Placeholders to fill out risk probabilities and impacts;
- Placeholder to identify the risk value (e.g., tolerable, acceptable).

The multi-objective risk matrix was concurrently developed by the industry partner and aligned with the overall company view on risk severity. The matrix included values for impact to the company and its customers.

Executing the workshops

Each workshop was attended by about 10 professionals, who discussed the selected case, and identified threats and their associated risks. Observers took notes and tracked time spent on specific tasks. Participants reflected at the end of each workshop on their learning's. Overall, the atmosphere of workshops was constructive and goal-oriented. Participants highlighted the importance to discuss and specify scope of application and context of the case.

The evaluation revealed challenges:

- There was no clear owner of the whole case scope;
- Some roles were assumed;
- Not everyone was aware of all parts of the system;
- The 1st case was rather open with diverse contexts across a range of customers;
- The 2nd case illustrated the complexity of compliance to both safety and security standards.

Findings included:

- It is crucial to clearly introduce the system and assessment scope;
- Need to explain domain specifics;
- Need to communicate the scope and skills of the expected attacker;
- Familiar visualization styles helps in aligning assessors;
- Time needed to absorb information on potential threats;
- Strong facilitation is required for time management and steering discussions during ranking;
- Ranking should consider impacts on both the customer and the supplier (high-tech company);
- Pre-read materials can help discussions on threats;
- Pre-workshop tasks, such as completing likelihood/impact tables, should be performed to reduce time spent justifying individual choices during the workshop;
- threat identification processes can be accelerated by considering common threats;
- A well-constructed DFD is highly beneficial (experts noted that 'having a good arch view is 80% of success').

Time tracking provided additional insights:

- The case introduction took about 15 minutes;
- Discussions of individual threats initially took about 15 minutes per threat, but then the process was speeding up, as the case boundary and context was better understood by all.

Observations and discussion

The participants recognized the flow of activities, their importance, and relevance to product development.

The key findings from the workshops include identified needs for:

› TNO Public › TNO 2026 R10857

- Thorough preparation: DFD and context construction; Template preparation; Clear role definition.
- Strong facilitation when workshops are used as a technique;
- Involving system and solution architects early;
- Allocating time for constructing a shared understanding;
- Clearly document threats for re-use in the later life cycle phases (e.g., in services phase).

Addressing these needs will benefit speeding up risk assessment activities.

The observations were shared with and confirmed by the company professionals involved in the study.

3. Conclusions and Future Work

Vanderlande delivers customer-specific solutions that consist of a combination of IACS products, as defined in IEC 62443 [8], and IT systems providing additional (cloud based) services. Both products and IT systems can have tiered supplier products as parts and can be integrated with third party products to realize a customer solution. These third party products can be delivered by Vanderlande as part of the solution or existing third party products at the customers. Because of the shift towards more interconnected CPS solutions, a holistic approach for risk assessments is needed, considering both OT and IT in the solution and in the context of the solution.

Vanderlande may perform the roles of both a product supplier and service provider, providing integration and/or maintenance services for respectively integrating and sustaining their supplied products in the environment of the asset owner (customer).

To verify the methodology, the security risk assessments were performed for two use cases: Digital Readiness, that includes IT, and Safety Instrumented System, that includes both IT and OT. A suitable use case for performing a trade-study on architecture alternatives was not found within the constraints of the project. The methodology as a whole could therefore not be validated. However, opportunities that "reusable assets" might bring in saving time and resources, and improving the quality of decision making were identified.

Conclusions

Based on the results of phase 1, the following conclusions were drawn:

- When calculating risk values, both the perspective of the product supplier and the customers owning the asset(s) should be considered. As risk appetite is defined independently by each organisation, it could be that the value is acceptable for one, but unacceptable for the other.
- Risk management benefits from reuse of threat information across the lifecycle, as assessments needs to be performed an updated frequently over the lifecycle. Reuse requires a managed, formal approach, where threat models and security risk files are updated and shared between the different risk owners over the life cycle.
- Updated threat intelligence requires feedback to earlier lifecycle phases, whereas a detailed threat model and context might result in an updated security risk file.
- As products are delivered world-wide to different customers; domain, country and market specific classifications should be supported. The actual system context only becomes clear when defined as part of a customer solution. In addition, the context can change over the lifecycle. For 'products in development', the worst-case value should be applicable.

The research questions were revisited after completion of phase 2. Answers to all research questions are given in the table below:

ID	Research Question and Answer
1	<i>How to architect for a continuous, adaptive cyber-risk management approach for the complete lifetime of automated cyber-physical systems, in balance with value-oriented system qualities to sustain customer value and operational continuity?</i> In cyber-physical systems, security is about engineering for intended and authorized system behavior and outcomes, despite anticipated and unanticipated adversity, conditions that may cause loss (e.g., threats, attacks, hazards, disruptions, exposures). This goes beyond information security, which itself already needs to balance multiple competing objectives like Confidentiality, Availability and Integrity and is also moving to loss of value and safety in its risk management. As security cannot be bolted on later but must be inherent in the design (secure-by-design), this requires continuous integration of the security in the SE workflow. The methodology therefore introduces a structured approach where trade-studies with Multi-Objective Decision Analysis and Decision Management are combined with risk assessment on alternatives created during architecting ensuring the right balance of risk and value. Threat modeling (from security domain) and STPA (from Systems Engineering domain) are both suitable approaches that include the analysis of unsafe control actions and system-level

interactions. These methods should also be used in concept definition, where the operational analysis is done, and system and trust boundaries are defined.

- 1.1 *How to improve security risk assessment for cyber-physical systems (CPS) in terms of execution speed, while maintaining quality and be applicable to all solution phases (development, project and services)*

By separating generic product assessments based on both supplier needs and the strictest target customer and country needs from the specific application/solution assessments for each individual customer. The generic product assessments serve as input to the solution assessments for both projects and services facilitating updates of solution risk assessments when products are updated.

- 1.1.1 *What can be automated and what needs a human (domain expert) in the loop?*

Calculating the risk value based on a business specific multi-objective risk matrix and the aggregated stakeholder value on a business specific multi-objective function can be automated. Estimating the risk values can be supported by automation based on historical data. Propagating risk outcomes from products to solutions containing those products can be supported by automation. The use of Multi-Objective Decision Analysis is especially relevant for security, as security is a composite objective with multiple conflicting subobjectives like confidentiality, integrity and availability. Defining the objectives and the actual decisions require human in the loop.

- 1.1.2 *When to go for empirical or creative methods for identifying threats?*

By capturing information in a reusable way, both historical empirical threat information and creative threat information will be available in many situations (updating is always easier than starting from scratch). Only for new concepts and new domains such information may not be available: in those cases make it dependent on the level of confidence needed for the decision which methods to apply and to what depth.

- 1.1.3 *When to go for quantitative or qualitative methods for determining security risks?*

Quantitative methods are preferred but require that likelihood and impact can be determined as well-defined in numerical values, for example through analysis or through historic information. Qualitative methods are needed when it is not possible to reliably estimate likelihood (e.g., lack of data), when the impact cannot be quantified (e.g., reputational damage), and under time and resource constraints.

- 1.2 *How to perform trade studies during development, based on risk assessment results from all solution phases?*

A decision management process should be defined that covers both product and solution lifecycle, and includes risk management and measurements.

- 1.2.1 *When to go for knowledge, skill or rule based decision making on enhancing security controls?*

Knowledge-based: developing multi-objective function and risk matrix, because it needs knowledge about the business or eco-system and application domain(s); Rule-based: trade-study, because solution specific information needs to be added or checked by subject matter experts; Skill-based: calculating risks and aggregated stakeholder value, because this can be automated (trusted data provided from other activities).

- 1.2.2 *What information/data, competencies, methods, techniques, etc are needed to make a decision?*

Artefacts: objectives, criteria, alternatives, risks, decisions & measures; Primary Roles: CY, MO, SA/ST, TM; Competencies: CT, SM, CP, DM, RO; Methods: MODA combined with Threat modelling or STPA

How to measure the value of a model-based versus document-based approach for trade-studies and risk assessments?

Effectiveness of the methodology can be measured in: percentage of risks identified and treated per lifecycle stage or in other words the 'uncertaintyLevel' per milestone or toll gate. Efficiency of the methodology can be measured in: processTime, and FTE.

The uncertaintyLevel per approach can be calculated by: $100\% * (1 - \text{accumulated risk per lifecycle stage} / \text{identified risk over the total lifecycle})$.

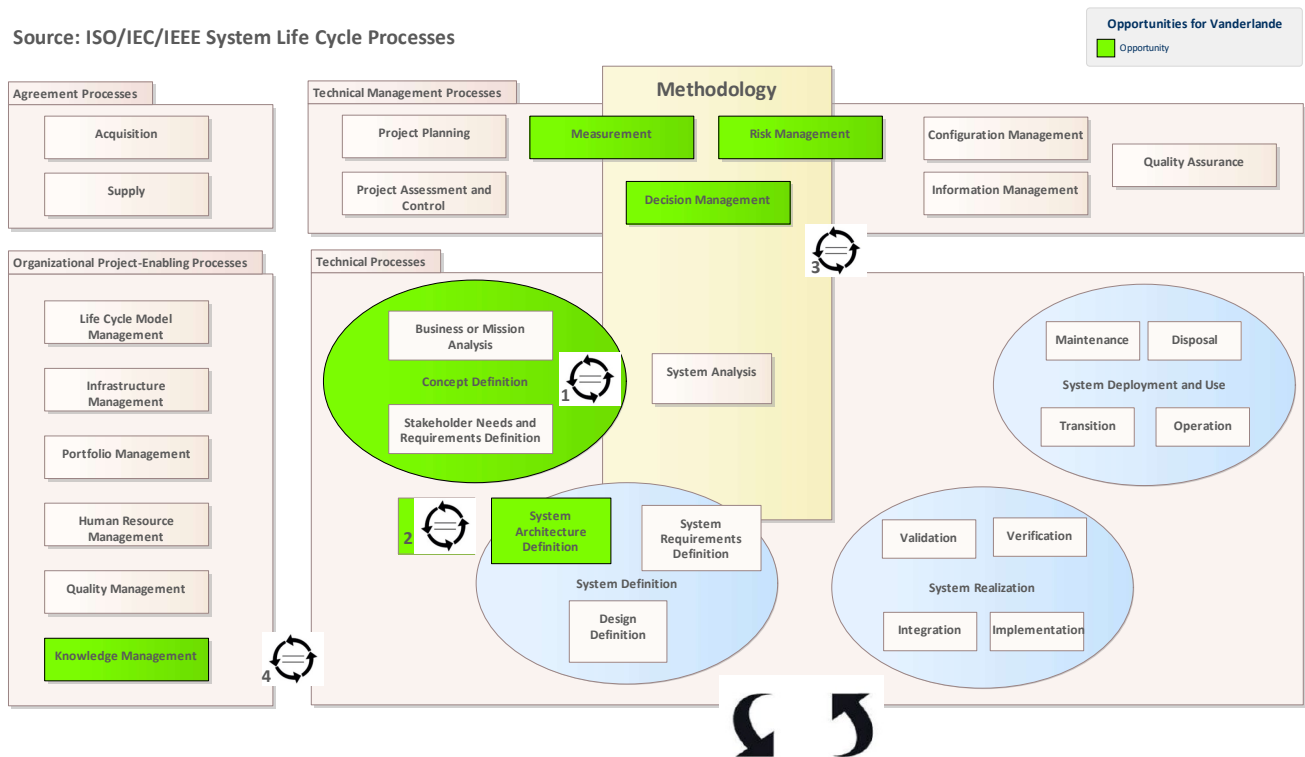


Figure 10: Opportunities in the Life Cycle Processes

Figure 10 highlights (in green markings) where opportunities were identified in the life cycle processes:

- Manage **knowledge assets** like multi-objective functions & risk matrices at organizational level;
- Manage **risks & decisions** across the entire lifecycle of both products and solutions;
- Manage operational concept definitions per application domain, including **objectives and measures of effectiveness**.

As part of the operational analysis (iteration 2), potential system architecture alternatives should be evaluated, and if needed (to prevent redesign) also be elaborated, taking unsafe control actions and system-level interactions into account. Threat modeling (from security domain) and STPA (from Systems Engineering domain) are both suitable approaches for such an analysis.

To summarize: evaluating alternative system architectures against multiple objectives will result in a simpler system than when an alternative is chosen and then updated multiple times in isolation because of risks with different objectives. The changes to the system because of these individual objectives will interfere with one another and with the aggregated stakeholder value. This methodology intends to prevent redesign by selecting the most feasible system architecture, taking into account the uncertainty (both risks and opportunities) in a holistic way.

Future Work

As a recommendation for future work the following is suggested:

- Apply the described methodology by comparing document-based with model-based approaches for preparing & performing trade studies and assessing risks;
- Identify additional drivers, challenges, and opportunities, including the state of practice, for the more regulated medical domain;
- Extend the scope from selecting system architecture alternatives towards design decisions that include technology and their maturity levels as part of customer-specific solutions;
- Evaluate STPA and Threat modelling (determine criteria for respectively system-level and security analysis);
- Validate (parts of) the methodology to an acceptable uncertainty level for making an implementation decision by multiple industry partners.

As a constraint "the 7 success factors" as described in [11] should be taken into account and no specific tools or notations should be developed (SysML and commercial tooling that supports this notation suffices).

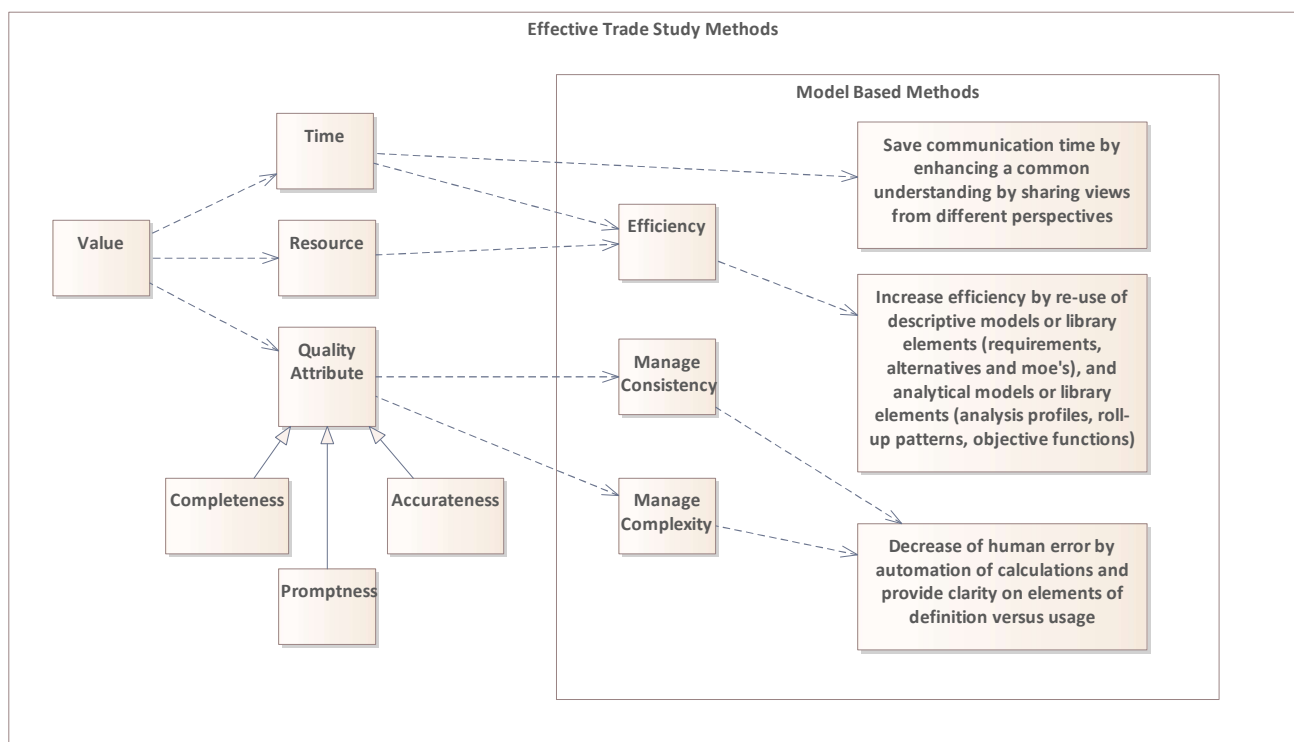


Figure 11: Measurements for an effective trade study

In general the value or "return of investment" of an effective trade study depends on:

1. Process time that can be saved for preparing and performing a trade study, but also for assessing the uncertainty that goes with a selected alternative, and processing the results of such a trade study;
2. Reduction of (critical) human resources (FTE's) that need to be in the loop, specifically for generating creative alternatives and assessing the risks associated with these alternatives. By only assessing selected alternative(s), the number of assessments can already be reduced;
3. Quality improvements in terms of completeness, accurateness and promptness. The result of a trade study should have an appropriate uncertainty level for the decision to make in the lifecycle of a product or solution. Using data on decisions, risks and measurements generated earlier in the lifecycle and data from comparable services, products or solutions lowers the uncertainty level.

A model-based approach may even further reduce process time, human resources, and improve quality:

1. Communication time can be saved by enhancing a common understanding by sharing views from system models and/or discipline specific models. A data flow diagram is a good example of representing a discipline specific model view that is very well recognised by security experts that are trained in threat modelling;
2. Both time and resources can be reduced by increasing efficiency by re-use of formalized data. Good

examples are concept definitions for both products and solutions. These definitions can be re-used in multiple projects. A concept definition for a product may even be reusable within multiple domains.

3. Quality can be improved by managing consistency and complexity. Using formalized data like a multi-objective risk matrix or multi-objective function for automation of calculations, human errors can be reduced and more clarity can be provided about the level of uncertainty.

An important prerequisite is that similar objectives and measures are used for selecting alternatives as for the risk assessments. The objectives should be smart enough to allow reasoning about measures of effectiveness and key performance measures (like done in Figure 11). The purpose of the model views should be very clear and people involved in creating and using the views should have the right competencies.

Reusable Assets

Most artefacts that are used or produced in preparing and performing a trade study or assessing risks are reusable assets. Some are domain agnostic, and some domain or context specific. The artefacts created in the SecureArch project, including this report, are created in a model and can be reused as inputs for future work.

Some examples of reusable assets:

- Concept definitions can be reused for multiple system (product or solution) definitions;
- Product definitions can be reused in multiple solution definitions;
- Objectives and their measures of effectiveness can be reused for multiple trade studies and risk assessments in a project;
- Combining objectives in a multi-objective risk matrix or function can be reused across multiple projects and products;
- Combining objectives for multiple domains in a multi-objective risk matrix or function can be reused across multiple business lines;
- Identified threats and threat models can be reused across projects, products, and solutions;
- The methodology as described in this report can be reused in multiple domains.

For this reason, some of the assets need to be managed at enterprise level, some at project level and some at product or service level. The lifecycle processes from ISO 15288 helps with a basic structure, but each organisation needs to augment these with the regulations and standards specific to their business, and tailor which asset to manage where to ensure the right information is available when needed.

System models (descriptive or analytical) and discipline-specific models can also be considered as reusable assets that automatically generate artefacts. For example, a threat model can generate a security risk file and a trade study model can automatically evaluate multiple alternatives. Both analytical models need a descriptive model of the system of interest.

4. Bibliography

ID	Source
[01]	INCOSE "Systems Engineering Body of Knowledge" definitions for Cyber-Physical Systems Available online: https://sebokwiki.org/wiki/Cyber-Physical_Systems_(glossary) [Accessed on: May 5, 2026].
[02]	INCOSE "SE Vision 2035" Available online: https://www.incose.org/resources-publications/technical-products/se-vision-2035/ [Accessed on: May 5, 2026].
[03]	ISO, Systems and software engineering - System life cycle processes, ISO/IEC/IEEE 15288, 2nd Edition 2023
[04]	"Cyber resilient system design methodology", TNO 2025 R1087, 30 April 2025
[05]	J. Holt and S. Perry "SysML for Systems Engineering - A Model-Based Approach", IET, 3rd Edition 2018
[06]	"Future proofing systems engineering competencies", TNO 2025 R2024-10169, 15 January 2025
[07]	INCOSE "Systems Engineering Handbook", INCOSE-TP-2003-002-05, 5th Edition 2023
[08]	IEC 62443 "International cybersecurity standards framework for operational technology (OT)"
[09]	S. Sheard and A. Pickard "Systems Engineering Roles for a New Era", INCOSE IS 2025
[10]	INCOSE Systems Engineering Body of Knowledge (SEBoK) "Decision Management" Available online: https://sebokwiki.org/wiki/Decision_Management [Accessed on: May 5, 2026].
[11]	J. Cederbladh and D. Krems "Successfully Integrating Early Validation and Verification in Industrial MBSE", INCOSE IS 2025
[12]	MITRE "The Trade Study Process" Available online: https://www.mitre.org/sites/default/files/2021-11/prs-21-0522-the-trade-study-process.pdf [Accessed on: May 5, 2026].
[13]	OWASP "Threat Modelling Process" Available online: https://owasp.org/www-community/Threat_Modeling_Process [Accessed on: May 5, 2026].
[14]	INCOSE Systems Engineering Competency Framework, 2nd Edition 2025
[15]	Buchanan, Scott Steele. Cyber-attacks to industrial control systems since Stuxnet: A systematic review. Capitol Technology University, 2022.
[16]	U.S. Congress. (2002). Homeland Security Act of 2002, Public Law, No. 107–296. U.S. Government Publishing Office. Available online: https://www.govinfo.gov/content/pkg/COMPS-1143/pdf/COMPS-1143.pdf [Accessed on: May 5, 2026].
[17]	European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, pp. 164–198. Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [Accessed on: May 5, 2026].
[18]	NIS2 directive. (2026). The NIS2 Directive Explained.

Available online:

<https://nis2directive.eu/postal-services/>

[Accessed on: May 5, 2026].

- [19] European Parliament & Council of the European Union. (2022a). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union.

Available online:

<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

[Accessed on: May 5, 2026].

- [20] European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

Available online:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>

[Accessed on: May 5, 2026].

- [21] European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/1230 of 14 June 2023 on machinery (Machinery Regulation). Official Journal of the European Union, L 165, pp. 1-102.

Available online:

<https://eur-lex.europa.eu/eli/reg/2023/1230/oj>

[Accessed on: May 5, 2026].

- [22] Center for Strategic and International Studies (CSIS). (2025). The PRC's evolving cyber laws and implications for Southeast Asia's digital economy and integration.

Available online:

<https://www.csis.org/blogs/new-perspectives-asia/prcs-evolving-cyber-laws-and-implications-southeast-asias-digital>

[Accessed on: May 5, 2026].

- [23] TNO "Vision and Outlook for Systems Architecting and Systems Engineering in the High-Tech Equipment Industry"

Available online:

<https://publications.tno.nl/publication/34642263/WXDoSj/TNO-2024-R10542.pdf>

[Accessed on: May 5, 2026].

- [24] Carnegie Mellon University "Architecture Tradeoff Analysis Method (ATAM)"

Available online:

<https://www.sei.cmu.edu/library/architecture-tradeoff-analysis-method-collection/>

[Accessed on: May 5, 2026].

- [25] Object Management Group "Risk Analysis And Assessment Modeling Language (RAAML)"

Available online:

[https://www.omg.org/spec/keyword/raaml,risk-analysis-and-assessment-modeling-language,safety,reliability,risk,hazard-analysis,stpa,systems-theoretic-process-analysis,fta,fault-tree-analysis,fmea,failure-mode-and-effects-analysis,gsn,goal-structured-notation,functional-safety,iso-26262,safety-of-the-intended-functionality,reliability-block-diagram,rbd,security](https://www.omg.org/spec/keyword/raaml,risk-analysis-and-assessment-modeling-language,safety,reliability,risk,hazard-analysis,stpa,systems-theoretic-process-analysis,fta,fault-tree-analysis,fmea,failure-mode-and-effects-analysis,gsn,goal-structured-notation,functional-safety,iso-26262,safety-of-the-intended-functionality,reliability-block-diagram,rbd,security/About-raaml,risk-analysis-and-assessment-modeling-language,safety,reliability,risk,hazard-analysis,stpa,systems-theoretic-process-analysis,fta,fault-tree-analysis,fmea,failure-mode-and-effects-analysis,gsn,goal-structured-notation,functional-safety,iso-26262,safety-of-the-intended-functionality,reliability-block-diagram,rbd,security)

[Accessed on: May 5, 2026].

- [26] Object Management Group "System Profile for Effective Cyber Threat-based Risk Assessments (SPECTRA)"

Available online:

<https://www.omg.org/spec/SPECTRA/>

[Accessed on: May 5, 2026].

Glossary

Term	Type	Meaning
Capability Engineering (CP)	SE Competency	An appreciation of the role the system of interest plays in the system of which it is a part
Critical Thinking (CT)	SE Competency	The objective analysis and evaluation of a topic in order to form a judgement
Data Flow	DFD concept	The data flow shape represents data movement within the application. The direction of the data movement is represented by the arrow.
Data Store	DFD concept	The data store shape is used to represent locations where data is stored. Data stores do not modify the data, they only store data.
Decision Management (DM)	SE Competency	The structured, analytical framework for objectively identifying, characterizing and evaluating a set of alternatives
External Entity	DFD concept	The external entity shape is used to represent any entity outside the application that interacts with the application via an entry point.
FailureMode	Situation	The manner in which a system or part of a system (e.g., functions, components, hardware, software, hardware parts, software units), can fail.
Hazard	Situation	Any situation that could contribute to an accident. Hazards should be eliminated wherever 'practicable', but this is not always the case. Where a hazard cannot be completely eliminated then there will be some risk.
Process	DFD concept	The process shape represents a task that handles data within the application. The task may process the data or perform an action based on the data. Note: A multiple process shape can be used to present a collection of subprocesses. The multiple process can be broken down into its subprocesses in another DFD.
Risk	Measure	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST]
Risk and Opportunity Management (RO)	SE Competency	The identification and reduction in the probability of uncertain events, or maximizing the potential of opportunities provided by them
Security Engineer (CY)	SE Role	Ensures security protection of entire system is given due consideration throughout system lifecycle certification and accreditation
Stakeholder Interface Manager (ST)	SE Role	Responsible for clear understanding between organization and stakeholders. Communication of perspectives, viewpoints, needs, changes, etc. Including how system will fit with stakeholders' existing systems.
System Architect (SA)	SE Role	Creates high level architecture and design. Selects major components. Selects and investigates alternative architectures. Ensures system works for context.
System Modeler (MO)	SE Role	Curator of system models, most being computer models
Systems Modeling and Analysis (SM)	SE Competency	Provision of rigorous data and information including the use of modeling to support technical understanding and decision making
Technical Manager (TM)	SE Role	Technical arm of project manager. Overseer of technical decisions among domains and across geographically dispersed teams. Manage risks with resource allocation
Threat	Situation	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access,

		destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [NIST]
Trust Boundary	DFD concept	The privilege boundary (or trust boundary) shape is used to represent the change of trust levels as the data flows through the application. Boundaries show any location where the level of trust changes.
Vulnerability	Situation	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [NIST]

Appendices

State of Practice investigation for trade-off analysis

3 Semi structured interviews were conducted in Q4 of 2025 and early 2026 with architects in 2 companies in high tech equipment industry that are ESI partners.

The purpose was to understand the current state of practice regarding trade-off analysis, e.g.

- Is a formal process or standard followed?
- What criteria are typically considered (e.g. cost, performance, risk, sustainability, security, etc)?
- How are conflicting objectives prioritized?
- Which tools or methods are used, including modelling and simulation?
- Who is involved in the analysis?
- How is it documented for future reference?
- What are the biggest challenges experienced in doing trade-off analysis?

1. Formal Process / Standards

- **No single formal standard** is consistently followed. Practices range from **systematic but lightweight methods** to **informal expert-driven approaches**.
- COMPANY A uses a Pugh-like method with weighted drivers for comparing variants—structured design process to address limited competing objectives but not a formal standard.
- COMPANY B uses **PowerPoint-based trade tables**, quantifying major aspects and risks, but process remains largely experience-driven rather than standards-driven.

2. Criteria Considered

Common criteria across companies include:

- **Performance** (e.g., throughput, performance)
- **Cost / Cost-of-goods**, including attempts to convert all impacts to euros for comparability (“apples to apples”).
- **Manufacturability & factory impact** (cycle time, required changes to factory).
- **Serviceability / Maintenance impact**.
- **Risk**, both technical and project risk; risk often difficult to quantify.
- **Sustainability aspects** (energy use, material usage such as tin, hydrogen).
- **Security & safety**, usually treated as boundary conditions rather than trade-off criteria.
- **Complexity**, scope of analysis and relations among criteria reduced as far as possible, focussed on performance rather than Measures of Effectiveness (MoEs)

3. Prioritizing Conflicting Objectives

- Conflicts are resolved by **explicit weighting** (e.g., Pugh matrix at Company A).
- At Company B, decisions focus on identifying the “pain points” per option and quantifying impacts to support comparison.
- Mandatory constraints (safety, basic security) eliminate options outright that don’t comply.
- When uncertainty is high, postpone decision or require additional studies / de-risking activities before selecting an option.

4. Tools & Methods Used

- **Decision matrices** (Pugh-like) for structured comparison.
- **Informal “menu card” comparisons** listing pros/cons (Company B, software focussed).
- **Discipline specific Analytical models** for quantification, e.g.: Cost models, CAD models, MATLAB performance models, CFD simulation models. It was found that system models were not used to consider the Measures of Effectiveness holistically
- **Risk burndown methods** exist but not tightly integrated into trade-off tables.
- **No automated or model-based decision frameworks** used for the trade-off itself (though interest exists).

5. People Involved

Trade-off decisions involved multiple stakeholders:

- Systems engineering & product architects (always involved).
- Design, engineering, manufacturing factories (across multiple international sites).
- Customer service & application engineers.
- Marketing → represents customer needs; customers do not participate directly.
- Sourcing & procurement, sometimes representing supplier feasibility.
- Program management / finance depending on context.

6. Information Management

- Document based: PowerPoint trade-off tables (Company B) are the primary artifact for decisions. Company A uses structured matrices, scores, and weights—likely stored in documents.
- Documentation includes stakeholder checks, ensuring that aspects from all disciplines are captured.
- Reuse of analytical models across generations is common, but reuse of decision rationale itself is limited; decisions rely heavily on human experience.

7. Major Challenges Identified

Across interviews the following challenges recur:

- High uncertainty early in projects → most difficult stage for making decisions.
- Quantifying impacts, especially: Risk, Cost (especially for future products), Performance estimates under uncertainty
- Balancing and enforcing many conflicting criteria while lacking uniform metrics.
- Limited formal risk quantification methods; quantifications often experiencebased rather than modelbased.
- Increasing complexity of systems, making trade-offs harder and more cross-disciplinary.
- Security as a moving target—treated as boundary condition, but evolving threats complicate design.
- Reuse of decision logic is minimal; decisions remain bespoke despite repeated patterns.