Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26537-cd

A Co-Analysis Framework for Safety and Cybersecurity Assessment in Autonomous Maritime Operations

Konstantinos Louzis

National Technical University of Athens, Greece. E-mail: klouzis@mail.ntua.gr

Panayiotis Siokouros

National Technical University of Athens, Greece. E-mail: panayiotis_siokouros@mail.ntua.gr

Reda Yaich

IRT SystemX, French Institute of Technology, France. E-mail: reda.yaich@irt-systemx.fr

Anastasia Danopoulou

National Technical University of Athens, Greece. E-mail: anastasiadan@mail.ntua.gr

This paper presents the results of a co-analysis framework for the integrated assessment of safety and cybersecurity in autonomous maritime operations. Developed within the context of the EC-funded SEAMLESS project, the framework addresses the critical challenge of analysing cascading effects in which cybersecurity breaches induce safety hazards and, conversely, safety-related failures create or amplify cyber vulnerabilities. The proposed methodology relies on the parallel execution of the EBIOS Risk Manager and STPA-SafeSec methodologies, using a phase-by-phase alignment to combine attacker-centric threat profiling with control-theoretic hazard analysis. This co-analysis enables the production of unified, traceable artefacts linking business assets and control components to threat actors and causal mechanisms. The framework has been developed and applied within SEAMLESS across autonomous port-operation use cases, including autonomous mooring and autonomous cargo handling. The paper presents detailed results for the autonomous cargo-handling use case, demonstrating the framework's ability to identify safety- and cybersecurity-relevant risk mechanisms, reveal coupled vulnerabilities, and support safe-and-secure-by-design development while strengthening operational resilience.

Keywords: Autonomous maritime systems, safety–security co-analysis, cyber-physical systems, cascading cyber–physical risk, STPA-SafeSec, EBIOS Risk Manager.

1. Introduction

The maritime industry is undergoing rapid digital transformation through autonomy, IoT connectivity, and advanced automation in port and vessel operations (Harish et al., 2024; Kouroupis & Sotiropoulos, 2024). These developments increase operational efficiency but also introduce new risk classes due to tight coupling between software, hardware, communication networks, and remote supervision (Mai et al., 2025). As OT becomes increasingly interconnected with IT, port infrastructures and vessels evolve into Cyber–Physical Systems (CPS) in which control decisions propagate through socio-technical control loops, blurring the boundary between safety incidents and cybersecurity breaches (Kouroupis & Sotiropoulos, 2024; Tabish & Chaur-Luh, 2024). In such environments, the traditional separation between safety incidents and cybersecurity breaches becomes blurred: cyber manipulation of data or control signals can directly induce hazardous physical behaviour, while safety-driven operational responses may introduce new cyber vulnerabilities (Harish et al., 2024; Kim, 2024). A central challenge for autonomous maritime operations is therefore the management of cascading cyber–physical risks, where disturbances originating in one domain propagate through interconnected control structures and result in failures in another (Danopoulou et al., 2025). Despite this

interdependence, safety and cybersecurity assessments are still commonly performed in isolation, limiting the ability to understand how cyber threats translate into hazardous system behaviour and how safety mechanisms may alter cyber risk exposure. This paper addresses this gap by proposing a co-analysis framework that integrates the EBIOS Risk Manager (EBIOS RM) methodology with STPA-SafeSec. Developed within the context of the SEAMLESS project, the framework enables the parallel execution of attacker-centric and system-theoretic analyses through phase-by-phase alignment, combining threat realism and prioritisation with rigorous control-structure reasoning. The proposed framework offers three main contributions: (1) a structured integration of EBIOS RM and STPA-SafeSec through phase-by-phase alignment, (2) explicit tracing of cascading risk propagation between cyber and physical domains, and (3) support for safe-and-secure-by-design system development through unified and auditable artefacts.

The framework is applied within SEAMLESS to multiple autonomous port-operation use cases, including autonomous mooring and autonomous cargo handling. This paper presents detailed results for the autonomous cargo-handling use case, illustrating how attacker-driven scenarios can be systematically linked to hazardous control actions and causal loss scenarios across safety and cybersecurity domains. The remainder of the paper presents the state of the art, the proposed co-analysis framework, its application, and the resulting findings and conclusions.

2. State of the Art

Recent literature highlights the limitations of treating safety and cybersecurity as separate concerns in autonomous CPS (Amorim et al., 2017; Kondeva et al., 2019; Mahsa Teimourikia, 2016; Pedroza, 2019). In highly automated maritime systems, cyber disturbances can propagate directly through control loops and lead to hazardous physical behaviour without classical component failures. Such tightly coupled cyber–physical interactions challenge the effectiveness of siloed assessment methodologies. Similar limitations have been reported across domains: in automotive CPS, safety and security mechanisms can introduce adverse cross-domain effects (Amorim et al., 2017; Bajan et al., 2022), while in maritime systems cyber threats have been shown to propagate through hierarchical control structures to produce hazardous outcomes (Danopoulou et al., 2025; Dghaym et al., 2021; Harish et al., 2024; Kouroupis & Sotiropoulos, 2024).

Existing approaches broadly follow co-analysis or co-engineering philosophies. Co-analysis combines safety and cybersecurity techniques (e.g., HARA/TARA extensions, FMVEA, SAHARA, STRIDE- or CORAS-based STPA-Sec adaptations) to jointly identify hazards and threats (Friedberg et al., 2017a, 2017b; Kaneko et al., 2019; Sahay et al., 2023; Shin et al., 2021; Temple et al., 2017). Co-engineering embeds both activities within unified workflows, iteratively re-evaluating cross-domain effects (Amorim et al., 2017; Kavallieratos et al., 2020; Kondeva et al., 2019; Navas et al., 2019; Temple et al., 2017).

Despite these advances, important gaps remain. Threat-centric cybersecurity methods provide structured reasoning about adversarial actions but typically lack explicit links to physical safety consequences and control-structure propagation. Conversely, system-theoretic approaches such as STPA and STPA-Sec effectively identify hazardous control actions and causal mechanisms, but under-represent attacker intent, exploitability, and confidentiality-driven compromise paths, and remain largely qualitative. As a result, existing methods do not systematically link cyber-attack realism to hazardous system behaviour. These limitations indicate the need for methodological complementarity rather than replacement. STPA-SafeSec provides a control-theoretic basis for

explaining how cyber disturbances lead to hazardous physical behaviour, while EBIOS RM, developed by ANSSI, offers an attacker-centric, scenario-driven cybersecurity framework structuring threat sources, strategic and operational scenarios, and treatment decisions (The French National Cybersecurity Agency (ANSSI), 2018). Aligning these methodologies enables coherent safety–security co-analysis while preserving traceability between cyber threats and safety-relevant control interactions.

3. Proposed Co-Analysis Framework

3.1. *Design Principles*

The proposed co-analysis framework integrates EBIOS RM and STPA-SafeSec through parallel execution on a shared system model, ensuring consistent system boundaries and aligned assumptions across safety and cybersecurity analyses. A key design principle is methodological complementarity: STPA-SafeSec provides control-structure-based identification of hazardous control actions and causal mechanisms within socio-technical control loops (Friedberg et al., 2017) while EBIOS RM contributes attacker-centric reasoning through risk origins and scenario-based cyber risk structuring.

The framework is explicitly designed to preserve the semantic integrity of both methodologies, avoiding the dilution of either system-theoretic causal reasoning or attacker-driven threat modelling. Rather than merging safety and cybersecurity into a single hybrid method, the framework aligns their execution to enable coherent interpretation of cross-domain effects.

3.2. *Methodology*

The framework is operationalised through a phase-by-phase alignment between EBIOS RM and STPA-SafeSec. Table 1 summarises the correspondence between analysis phases and expected outputs within the integrated workflow, including the alignment of business assets and feared events with system-level losses, and of cyber operational scenarios with causal loss scenarios.

A key integration point is the linkage between EBIOS RM operational scenarios and STPA-SafeSec causal loss scenarios: operational scenarios instantiate concrete cyber mechanisms (e.g., integrity, availability, or timing violations) that can drive process-model mismatches and trigger hazardous control behaviour. This alignment enables systematic traceability from attacker-driven scenarios to safety-relevant control failures and their potential physical consequences.

3.3. Documentation and Artefacts

The application of the proposed framework results in a deliberately limited set of structured artefacts supporting traceability across safety and cybersecurity analysis phases. For each analysed use case, a component-level control structure is defined, capturing the control relationships between supervisory controllers, autonomous control units, actuators, and the controlled physical process. This shared model provides the reference structure for both STPA-SafeSec and EBIOS RM analyses.

Within the scope of this paper, the control structure of the autonomous cargo-handling system is presented in Section 3 and serves as the basis for the subsequent co-analysis. The resulting artefacts enable explicit traceability from attacker-driven cyber scenarios to affected control components, process-model mismatches, hazardous control actions, and derived safety and security requirements.

By constraining the artefact set to those strictly required for cross-domain reasoning, the framework remains applicable in industrial contexts while preserving end-to-end analytical traceability.

Table 1. Phase-by-phase alignment of EBIOS Risk Manager and STPA-SafeSec within the co-analysis framework.

Phase	EBIOS RM	STPA-SafeSec	Output
Phase 1	Scope definition, essential services, business assets	Define purpose of analysis: unacceptable losses, system-level hazards, and system-level constraints	Aligned analysis boundary and safety–security objectives (loss/hazard framing for both domains)
Phase 2	Ecosystem analysis and identification of Risk Origins (threat actors)	Model the control structure: controllers/controlled processes, control actions, and process-model variables	Shared system model used to connect business assets/threat origins to control components and data flows
Phase 3	Strategic scenarios (high-level attack paths affecting assets/services)	Identify Hazardous Control Actions (HCAs), including those arising from security-compromised process-model conditions.	Traceability between strategic attack intent and unsafe control actions (which control actions could be rendered unsafe)
Phase 4	Operational scenarios (concrete technical mechanisms, attack steps)	Identify causal loss scenarios explaining how HCAs occur	Explicit cyber-to-safety and safety-to-cyber cascading paths at scenario level
Phase 5	Risk evaluation & treatment options	Derive controller-specific safety and security constraints and requirements	Unified set of implementable requirements mapped to scenarios, hazards, and constraints

4. Application and Results

4.1. SEAMLESS Use Cases

The proposed co-analysis framework was applied within the SEAMLESS project to autonomous port-operation use cases, including autonomous mooring and autonomous cargo handling. System descriptions and operational concepts are defined in SEAMLESS Deliverable D2.3 and are not repeated here. Both use cases were analysed using the same methodology; however, due to space limitations, detailed results are presented only for autonomous cargo handling, a safety-critical operation characterised by tightly coupled cyber–physical interactions and remote supervision. Results from the autonomous mooring use case inform the cross-case findings in Section 4.2. The analysis focuses on safety- and cybersecurity-relevant control structures, control actions, process-model variables, and operational scenarios. The following subsection presents the integrated STPA-SafeSec and EBIOS RM co-analysis results for autonomous cargo handling.

The STPA-SafeSec analysis of the autonomous cargo-handling operation produced a comprehensive set of safety–security artefacts across all analysis steps. Based on the defined control structure, the analysis identified 9 unacceptable losses and 11 system-level hazards, which were translated into 27 safety, integrity, and availability constraints addressing hazardous conditions related to crane motion, load control, human presence, environmental limits, situational awareness, and supervisory control. Fig. 1 presents the component-level control structure of the autonomous cargo-handling system used as the basis for the STPA-SafeSec and EBIOS RM co-analysis.

The structure comprises four interacting controllers—the Remote-Control Centre (RCC), Vessel Cargo Operation Platform (VCOP), Autonomous Crane Control Unit (CCU), and the crane actuation layer (CC3000).

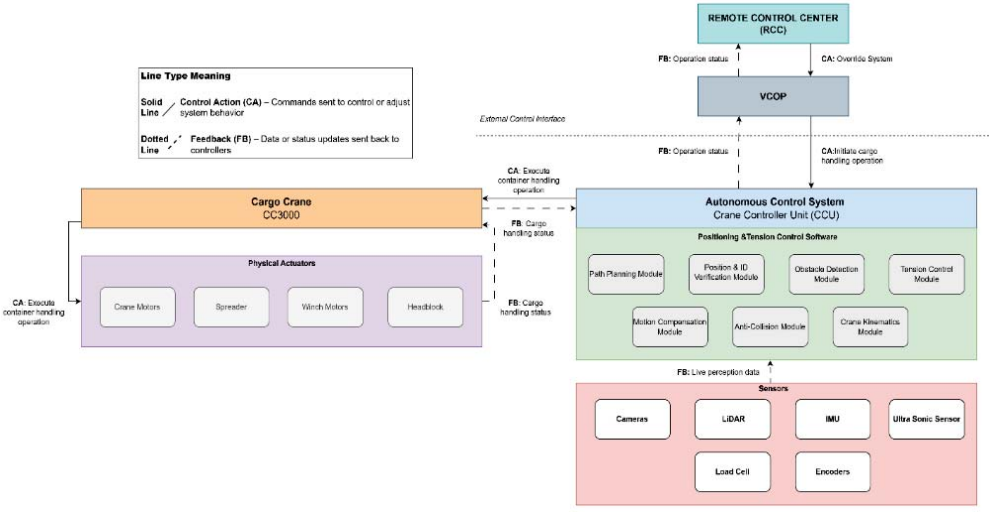

Fig. 1. Control structure of the autonomous cargo-handling system.

Across these controllers, 21 control actions and 14 process-model variables were defined, capturing operational phase, control mode, supervision availability, environmental envelope status, load-attachment state, actuator limits, and controller health.

From this model, 44 Hazardous Control Actions (HCAs) were identified, reflecting hazardous authorisation, inappropriate timing of crane or hoist commands, hazardous release or locking of the spreader, and continuation of autonomous operation under degraded or inconsistent feedback. Subsequent causal analysis resulted in the identification of 16 loss scenarios, which informed 34 controller-specific safety and security requirements. Notably, several HCAs and loss scenarios were only identifiable when integrity and timeliness violations were treated as process-model causal factors, demonstrating the added value of linking attacker-driven operational scenarios to control-structure reasoning.

To illustrate end-to-end causal reasoning, a representative chain is summarised for the Autonomous Crane Control Unit (CCU). An unacceptable loss involving injury or equipment damage is associated with a hazard in which the load is lifted or moved while not securely attached or while operating conditions exceed validated limits. This manifests as an HCA whereby the CCU commands hoisting or crane motion despite uncertain or incorrect load-attachment status or exceeded actuator limits. The corresponding loss scenario describes a mismatch between the CCU process model and the actual system state, potentially induced by spoofed or delayed attachment-status feedback or corrupted limit telemetry, leading to unstable load motion and excessive forces. The derived requirement enforces multi-source validation of load-attachment and actuator-limit status, integrity and freshness checks on feedback, and immediate transition to a safe state upon detection of inconsistencies. Within the co-analysis framework, attacker-driven operational scenarios identified through EBIOS RM were mapped to the control-structure elements and process-model conditions identified in the STPA-SafeSec analysis, enabling explicit tracing from cyber-attack realisation paths to hazardous control actions and safety-relevant loss scenarios.

In parallel, the EBIOS RM analysis provided a structured, business-driven assessment of cybersecurity risks affecting autonomous cargo handling, with particular focus on the convergence of port IT systems, autonomous crane control, remote operations, and cloud-based optimisation services. The analysis identified 5 primary feared events spanning safety, operational, economic, and information-centric impacts, evaluated across five impact categories using harmonised EBIOS RM severity scales.

Based on the threat ecosystem analysis, 6 categories of risk sources were retained, including cybercriminal groups, competitors, state-sponsored actors (APT), malicious insiders, and unintentional insiders. This resulted in 9 strategic risk scenarios, of which 6 were retained as critical. These scenarios capture attack logics such as ransomware-driven disruption of cargo operations, theft of optimisation data, long-term APT presence via the industrial supply chain, and sabotage of port automation infrastructure. Each retained strategic scenario was decomposed into two representative operational scenarios, yielding 12 operational scenarios describing credible attack paths across remote operations, IT/OT interconnections, third-party platforms (VCOP), insider access, and supply-chain dependencies. When mapped to the STPA-SafeSec results, these operational scenarios predominantly affected supervisory authorisation logic, feedback integrity, and mode-management decisions, directly corresponding to HCAs and loss scenarios identified in the control-theoretic analysis. The resulting risk picture informed the definition of five major cyber risks affecting autonomous cargo-handling operations, which were used to derive targeted treatment measures across governance, protection, detection, and resilience domains, aligned with safe-and-secure-by-design objectives.

4.2 Discussion

Across the autonomous mooring and cargo-handling use cases, the proposed co-analysis framework revealed systematic safety–cybersecurity coupling patterns that remain largely invisible to isolated safety or cybersecurity assessments. In both cases, safety-critical behaviour primarily arose from mismatches between controller process models and the actual system state, particularly under conditions of degraded supervision, delayed feedback, or integrity-compromised information. Supervisory and coordination controllers consistently emerged as key convergence points for cascading cyber–physical effects, as cyber-originating disturbances affecting data integrity, availability, or timeliness propagated through control structures and manifested as hazardous control actions with direct physical consequences. Conversely, safety-driven operational responses, such as degraded supervision or emergency mode transitions, were shown to introduce new cybersecurity exposures by modifying system configuration, trust relationships, or access assumptions, thereby confirming the inherently bidirectional nature of cascading risk. Despite differences in physical processes and operational objectives, consistent causal structures were identified across both use cases, including hazardous continuation of operation under inconsistent feedback, inappropriate timing or authorisation of control actions during mode transitions, and loss of situational awareness under degraded supervision. These recurring patterns indicate that safety–security coupling mechanisms are structural properties of autonomous port-operation control architectures rather than use-case-specific anomalies.

From a methodological perspective, the co-analysis demonstrated clear added value over isolated applications of STPA-SafeSec or EBIOS RM by explicitly grounding attacker-driven cyber scenarios in control-theoretic explanations

of hazardous physical behaviour. Rather than focusing solely on prevention of known threats, the resulting analysis supports a more resilience-oriented interpretation of safe-and-secure-by-design, in which safety constraints remain enforceable even under partial cyber compromise. The primary outcome is therefore a unified, prioritised, and traceable set of safety and security constraints that can be directly allocated to controllers and interfaces, supporting assurance arguments for both robust system design and resilient operation throughout the system lifecycle.

5. Conclusions

The results presented in Section 4 demonstrate that safety–cybersecurity coupling in autonomous port operations is structurally embedded in the interaction between distributed control architectures, remote supervision, and cyber-enabled information flows. By explicitly linking attacker-informed cyber scenarios to hazardous control actions and causal loss scenarios, the proposed co-analysis framework enables earlier and more coherent identification of coupled safety and cybersecurity vulnerabilities than isolated assessments. The contribution of this work does not lie in proposing a new safety or cybersecurity method, but in providing an explicit alignment mechanism that preserves the semantics of both STPA-SafeSec and EBIOS RM while enabling auditable cyber-to-safety traceability. This alignment grounds attacker realism and threat prioritisation in control-structure-based explanations of hazardous physical behaviour, addressing a key limitation of existing co-analysis approaches. At the same time, the framework requires interdisciplinary expertise and may generate a substantial volume of analysis artefacts without dedicated tool support, while the integration of semi-quantitative cybersecurity assessments with qualitative system-theoretic safety analysis remains methodologically challenging. Overall, this paper presented a co-analysis framework for the integrated assessment of safety and cybersecurity in autonomous maritime operations. Application to autonomous mooring and autonomous cargo-handling use cases demonstrated the framework's ability to systematically link threat-driven cyber scenarios to hazardous control behaviour, causal loss scenarios, and controller-specific requirements, confirming that process-model mismatches, particularly under degraded supervision or compromised information, are central drivers of safety-critical outcomes.

Future work will extend the application of the framework to additional autonomous maritime operations and explore its integration with industrial design, assurance, and verification workflows, as well as the use of quantitative and semi-quantitative techniques to support scenario prioritisation and further examine cyber-to-safety causal pathways.

Acknowledgement

The work presented in this paper is in the context of the SEAMLESS project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101096923.

References

Amorim, T., Martin, H., Ma, Z., Schmittner, C., Schneider, D., Macher, G., Winkler, B., Krammer, M., & Kreiner, C. (2017). Systematic Pattern Approach for Safety and Security Co-engineering in the Automotive Domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10488 LNCS*, 329–342. https://doi.org/10.1007/978-3-319-66266-4_22

Bajan, P. M., Boyer, M., Dubois, A., Letailleur, J., Mantissa, K., Sobieraj, J., & Tlig, M. (2022). Proposal of Cybersecurity and Safety Co-engineering Approaches on Cyber-Physical Systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13414 LNCS*, 175–188. https://doi.org/10.1007/978-3-031-14835-4_12

Danopoulou, A., Georgantopoulos, P., Ventikos, N. P., & Louzis, K. (2025). Assessing Cascading Cybersecurity and Safety Risks in Autonomous Maritime Operations. *Proceedings of the 2025 Annual Conference of Marine Technology*.

Dghaym, D., Hoang, T. S., Turnock, S. R., Butler, M., Downes, J., & Pritchard, B. (2021). An STPA-based formal composition framework for trustworthy autonomous maritime systems. *Safety Science*, *136*, 105139. https://doi.org/10.1016/j.ssci.2020.105139

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017a). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, *34*, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2017b). STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems. *Journal of Information Security and Applications*, *34*, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008

Harish, A. V, Tam, K., & Jones, K. (2024). Literature Review of Maritime Cyber Security: The First Decade. *Maritime Technology and Research*, *7*(2), 273805. https://doi.org/10.33175/mtr.2025.273805

Kaneko, T., Sasaki, R., & Takahashi, Y. (2019). *Threat analysis using STRIDE with STAMP/STPA*.

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2020). Cybersecurity and safety co-engineering of cyberphysical systems - A comprehensive survey. *Future Internet*, *12*(4). https://doi.org/10.3390/FI12040065

Kim, S. K. (2024). An Approach to Maritime Cyber Security Risks: Nature and Countermeasures. *The International Journal of Marine and Coastal Law*, *40*(1), 181–202. https://doi.org/10.1163/15718085-bja10200

Kondeva, A., Nigam, V., Ruess, H., & Carlan, C. (2019). On Computer-Aided Techniques for Supporting Safety and Security Co-Engineering. *2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 346–353. https://doi.org/10.1109/ISSREW.2019.00095

Kouroupis, K., & Sotiropoulos, L. (2024). Cyber Challenges amid the Digital Revolution in Maritime Transport. *Juridical Tribune - Review of Comparative and International Law*, *14*(2), 321–340.

Mahsa Teimourikia. (2016). *Co-Engineering Safety and Security in Risk-Prone Smart Work Environments*.

Mai, V.-T., Mohammadzadeh, A., Alattas, K. A., Taghavifar, H., & Ghaderpour, E. (2025). Cybersecurity in Maritime Power Systems: A Comprehensive Review of Cyber Threats and Mitigation Techniques. *Electric Power Systems Research*, *247*, 111797. https://doi.org/10.1016/j.epsr.2025.111797

Navas, J., Voirin, J.-L., Paul, S., & Bonnet, S. (2019). *Towards a Model-Based approach to Systems and Cyber Security co-engineering*.

Pedroza, G. (2019). *Towards Safety and Security Co-engineering Towards safety and security co-engineering Challenging aspects for a consistent intertwining*. 10. https://doi.org/10.1007/978-3-030-16874-2ï

Sahay, R., Estay, D. A. S., Meng, W., Jensen, C. D., & Barfod, M. B. (2023). A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103179

Shin, J., Choi, J. G., Lee, J. W., Lee, C. K., Song, J. G., & Son, J. Y. (2021). Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed. *Nuclear Engineering and Technology*, *53*(10), 3319–3326. https://doi.org/10.1016/j.net.2021.04.031

Tabish, N., & Chaur-Luh, T. (2024). Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. *IEEE Access*, *12*, 17114–17136. https://doi.org/10.1109/ACCESS.2024.3357082

Temple, W. G., Wu, Y., Chen, B., & Kalbarczyk, Z. (2017). Reconciling Systems-Theoretic and Component-Centric Methods for Safety and Security Co-analysis. In *Computer Safety, Reliability, and Security Print ISBN: 978-3-319-66283-1 Electronic ISBN: 978-3-319-66284-8* (pp. 87–93). https://doi.org/10.1007/978-3-319-66284-8_9

The French National Cybersecurity Agency (ANSSI). (2018). *La méthode EBIOS Risk Manager — ANSSI*. https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/