Operationalising Compliance in Manufacturing: Applying the FAST Method to NIS2 and the CRA

Vjatšeslav Antipenko[1,*], Raimundas Matulevičius[1]

[1]*University of Tartu, Ülikooli 18, 50090 Tartu, Estonia*

Abstract

Industrial organisations face increasing pressure to comply with evolving security regulations, including the NIS2 Directive (NIS2) and the Cyber Resilience Act (CRA). Yet translating legal obligations into operational practices remains a persistent challenge, especially for manufacturers in automated environments. This paper addresses this gap by aligning the FAST method —a function-driven threat modelling method for identifying and treating security threats—with obligations extracted from NIS2 and CRA. We elicit, classify, and refine regulatory requirements into acceptance criteria, mapping them to FAST artefacts using a requirements engineering approach grounded in Breaux and Antón's methodology. The resulting compliance artefact was validated through expert feedback. Our findings demonstrate that FAST provides a viable pathway for operationalising regulatory compliance through function- and asset-level risk analysis, offering a foundation for future implementation and audit readiness.[1]

Keywords

security compliance, NIS2 Directive, Cyber Resilience Act, risk management, industrial automation, regulatory engineering, FAST method,

1. Introduction

The digitalisation of industrial operations has transformed manufacturing, integrating automation, connected supply chains, and real-time data to sustain competitiveness [1]. Yet this connectivity exposes production environments to increasingly sophisticated cyber threats [2].

Unlike conventional IT systems, manufacturing relies on complex cyber-physical infrastructures that are often built on legacy technology [3, 4]. Further convergence of IT and Operational Technology (OT) has expanded the attack surface, allowing digital compromises to disrupt physical processes [5]. As a result, industrial incidents now cause both financial and operational harm [6].

To address these risks, the European Union enacted Directive (EU) 2022/2555 (NIS2) [7] and Regulation (EU) 2024/2847 (CRA) [8]. Together, they require risk-based measures covering but not limited to incident response, business continuity, supply-chain assurance, and vulnerability management [9]. While establishing a foundation for resilience, they also impose demanding

[1] The compliance artefact, including requirement datasets and FAST mappings, is publicly available at Zenodo: https://doi.org/10.5281/zenodo.15663474

PoEM2025: Companion Proceedings of the 18th IFIP Working Conference on the Practice of Enterprise Modeling: PoEM Forum, Doctoral Consortium, Business Case and Tool Forum, Workshops, December 3-5, 2025, Geneva, Switzerland

[*] Corresponding author.

vjatseslav.antipenko@ut.ee (V. Antipenko); rma@ut.ee (R. Matulevičius)
0009-0007-8032-963X (V. Antipenko); 0000-0002-1829-4794 (R. Matulevičius)

compliance obligations [10].

Despite growing attention, translating these high-level legal requirements into practical industrial applications remains challenging. Existing case studies focus mainly on sectors such as healthcare or digital services [11, 12], leaving manufacturers with limited guidance on aligning production systems and governance processes with NIS2 and CRA expectations. Addressing this gap is essential for both compliance and the long-term resilience of automated manufacturing.

1.1. Research Challenge

Manufacturers face the task of interpreting general security obligations within highly specialised, multi-vendor, and often legacy environments [13]. Standards such as IEC 62443 provide partial coverage but do not fully reflect the extended responsibilities introduced by NIS2 and CRA [1].

Given this, the study asks:

How can manufacturing organisations address security risks to ensure compliance with NIS2 and CRA?

Rather than introducing a new framework, we explore how the existing FAST method (Functions, Assets, Security Threats, Treatments) [14] can be applied as a practical compliance method. FAST structures risk identification and mitigation in cyber-physical systems, offering a basis for aligning manufacturing security practices with regulatory requirements.

The remainder of this paper is organised as follows: Section 2 summarises the regulatory and methodological background; Section 3 outlines the compliance validation process; Section 4 presents results; Section 5 reports expert feedback; and Section 6 concludes with reflections and future work.

2. Background

This section outlines the regulatory context of NIS2 and the CRA and introduces the FAST method, which is subsequently evaluated for its compliance with these regulations.

2.1. Security Regulations: NIS2 and CRA

Directive 2022/2555 (NIS2) and Regulation 2024/2847 (CRA) jointly define security requirements across EU critical sectors. NIS2 focuses on organisational risk management for essential and important entities, while CRA targets product-level security for manufacturers, importers, and distributors. Together, they aim to establish a coherent European security posture.

For manufacturers, NIS2 obligations include risk analysis, incident reporting, business continuity, and supply-chain security [15]. CRA extends these to secure-by-design product development, vulnerability management, and documentation of security features [16]. In practice, product and process boundaries overlap: vulnerabilities in embedded devices can endanger entire production systems [10].

Although both frameworks promote proactive, risk-based governance, practical guidance for manufacturers is still limited. Existing examples emphasise other domains [11], leaving companies to interpret broad legal principles within complex industrial settings [17, 18].

2.2. The FAST Method

FAST is a method for analysing and mitigating security risks in industrial automation and cyber-physical systems [14, 19]. Rather than redefining risk management and threat modelling, it organises existing practices around information processing functions and their supporting assets. The method comprises four components (Figure 1):

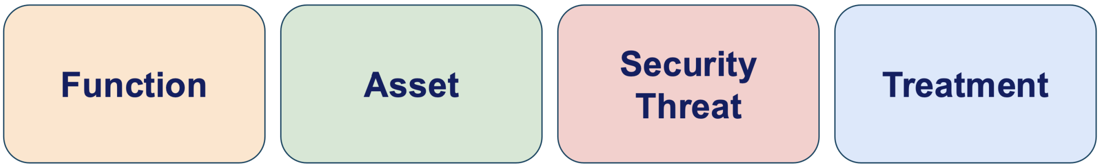

Figure 1: The FAST Method

- ***Functions*** – Derived from Alter's Work System Model [20], describing how systems capture, transmit, store, retrieve, manipulate, and display information.
- ***Assets*** – Classified following ISSRM principles [21, 22], covering technological and business assets. Asset classification also informs the *Risk Management Plan* (R), which formalises governance and escalation processes.
- ***Security Threats*** – Identified using STRIDE [23] and MITRE ATT&CK for ICS [24], supporting exposure analysis.
- ***Treatments*** – Mitigation measures selected by feasibility and impact to address identified threats.

FAST clarifies how information-processing functions expose assets to attack vectors and guides the design of targeted countermeasures. FAST produces artefacts—such as threat matrices, risk classifications, and mitigation plans—that correspond to activities required by security regulations. Consequently, this study examines the extent to which applying FAST enables an organisation to achieve regulatory compliance in manufacturing contexts.

3. Compliance Validation Method

This section outlines the validation method used to determine whether FAST outputs fulfil security obligations under the NIS2 Directive and the Cyber Resilience Act. The method adapts established legal-requirement extraction techniques to the manufacturing domain and follows a seven-step process: from acquiring and analysing legal text to defining acceptance criteria and mapping them to FAST components and artefacts. All extracted requirements, classifications, and mappings are publicly available at Zenodo[1].

3.1. Foundations — Adapting Breaux & Antón

The compliance validation process implemented in this study draws upon the regulatory analysis method proposed by Breaux and Antón (2008) [25], originally designed for extracting rights, obligations, and constraints from privacy and security laws such as HIPAA. The method was selected for its ability to:

- Decompose legal text into semantic components (e.g., obligation, right, constraint, exception),
- Preserve clause-level traceability,
- Handle legal complexity such as cross-references and conditional duties,
- Translate legal language into actionable, system-relevant requirements.

Given the layered and actor-specific structure of NIS2 and CRA, a method with these capabilities is essential. Table 1 compares this approach with alternatives.

Table 1
Comparison of Methods for Legal Requirement Extraction and Compliance Mapping

Authors	**Breaux & Antón (2008)** [25]	**Zarrabi et al. (2011)** [26]	**Fatema et al. (2016)** [27]	**Islam et al. (2010)** [28]
Focus	Extracting *privacy & security obligations* from legal texts	Mapping *legal obligations to security system models*	*Automating access control enforcement* from laws	Managing *security/privacy requirements over time*
Key Methodology	*Semantic parameterisation* (rights, obligations, constraints, exceptions)	*Hohfeld's Legal Taxonomy + Secure Tropos*	*Controlled Natural Language (CNL) + XACML/PERMIS*	*Secure Tropos + Goal-Driven Risk Management (GSRM)*
Suitability for FAST Compliance Validation	Strong fit due to role-based traceability	Needs extra validation layer	Not applicable	May support future-oriented extensions

3.1.1. Expansions to the Validation Method

To tailor the Breaux & Antón method for security regulation in manufacturing, three targeted adaptations were introduced.

(1) Role-Based Filtering: Only obligations relevant to private-sector entities—manufacturers, importers, and operators of essential or important services—were retained, excluding state-level policy duties except where they indirectly affect manufacturers.

(2) Extended Keyword Set: The extraction logic was expanded beyond legal verbs (*shall*, *must*) to include domain-specific terms such as *mitigate*, *govern*, and *assess*, capturing the technical language common in security legislation.

[1] https://doi.org/10.5281/zenodo.15663474

(3) FAST Alignment: Each obligation was linked to relevant FAST components—Function (F), Asset (A), Security Threat (S), Treatment (T), or Risk Management Plan (R)—and corresponding artefacts. This enables compliance traceability and evidence-based validation during audits.

Together, these refinements operationalise a transparent and domain-aware compliance pipeline.

3.1.2. Compliance Processing Pipeline

The compliance pipeline operationalises the adapted Breaux & Antón method as a seven-step procedure that converts regulatory clauses into testable criteria mapped to FAST artefacts. The process was implemented through structured text extraction, spreadsheet analysis, and expert verification to maintain traceability (Table 2).

Table 2
Seven-Step FAST Compliance Validation Pipeline

Step	Action	Implementation and Output
1	Acquire legal texts	NIS2 and CRA versions retrieved from EUR-Lex and segmented by article and paragraph.
2	Extract requirements	Clauses describing obligations, rights, or constraints recorded in a tabular dataset.
3	Filter by role	Rule-based selection retained items relevant to manufacturers, importers, and operators of essential or important services.
4	Classify	Each obligation categorised using Firesmith's [29] security taxonomy.
5	Define criteria	Acceptance criteria formulated as measurable statements derived directly from requirement text.
6	Map to FAST	Criteria linked to FAST components—Function (F), Asset (A), Security Threat (S), Treatment (T), or Risk Management Plan (R)—and to corresponding artefacts.
7	Assess coverage	Each criterion assigned a coverage value: full, partial, conditional, or none, with rationale recorded in the dataset.

FAST artefacts used in step 6, mapping include the threat matrix, asset inventory, control catalogue, mitigation plan, and residual-risk register. These outputs represent evidence that can be reviewed or audited against legal obligations. Coverage categories, used in step 7, describe how completely each legal criterion is addressed within FAST: *fully covered* (criterion satisfied), *partially covered* (criterion addressed in part), *conditionally covered* (criterion handled through the Risk Management Plan), and *not covered* (criterion outside current FAST scope). All classifications include explicit references to the artefacts used in the assessment.

3.2. Threats to Validity

The validation process has several limitations considered across four dimensions: construct, internal, external, and reliability.

Construct validity concerns whether the study captures security compliance in full. To cover legal, technical, and organisational aspects, the extraction used an extended keyword set and role-based filtering. All identified obligations and criteria were jointly reviewed to ensure consistent interpretation.

Internal validity relates to whether mappings between legal criteria and FAST components result from the method rather than bias. Mappings followed predefined rules linking requirement types to FAST elements and were checked by multiple coders until agreement was reached. Items outside the FAST scope were recorded under the Risk Management Plan (R).

External validity addresses generalisability. Results reflect the manufacturing context and should be replicated in other industrial settings before extending the method to additional frameworks such as ISO/IEC 27001 or IEC 62443.

Reliability concerns repeatability. All sources were version-controlled, and the extraction and mapping rules were documented to allow independent replication.

4. Findings

This section presents the results of the compliance validation analysis, focusing on the alignment between obligations defined in the NIS2 Directive and the Cyber Resilience Act and the outputs generated by the FAST method. The analysis relies on the traceability model described below, which links legal obligations—through derived acceptance criteria—to FAST components and artefacts. The complete dataset, including extracted requirements, classifications, and mappings, is available at Zenodo[2].

4.1. Scope of Extracted Obligations and Criteria Development

Using the keyword and role-filtering methods from Section 3, we identified **253 obligations in NIS2** and **342 in CRA**. Many concern national authorities or enforcement mechanisms and were therefore excluded. After filtering for manufacturing-relevant roles such as manufacturers, suppliers, importers, and essential entities, **40 NIS2** and **96 CRA** obligations remained for assessment.

Each obligation was decomposed into one or more **acceptance criteria**, yielding over **160 testable statements**. The number per obligation depended on clause complexity: simple requirements produced a single criterion, while compound or conditional clauses were divided into multiple items.

4.2. Compliance Traceability Framework

The compliance traceability framework links each regulatory requirement to the FAST components and artefacts demonstrating its fulfilment. Each requirement receives a unique legal reference (e.g., CRA-13-2) and is translated into measurable acceptance criteria. These criteria are mapped to relevant FAST elements—Function (F), Asset (A), Security Threat (S), Treatment (T), or Risk Management Plan (R)—and to the artefacts created during implementation. For each mapping, the coverage level (*fully*, *partially*, *conditionally*, or *not covered*) and a concise justification are recorded. Together, these form the compliance validation matrix in Table 3, providing traceability from legal text to system-level evidence.

[2] https://doi.org/10.5281/zenodo.15663474

Table 3
Illustrative Compliance Validation Matrix

ID	Acceptance Criterion	FAST Component(s)	FAST Artefact(s)	Coverage Status	Justification
CRA-13-2	The manufacturer shall update the security risk assessment throughout the product lifecycle.	A, T, R	FA-02, FA-03, FA-05	Fully Covered	Risk assessments are continuously updated as part of FAST's treatment selection and risk evaluation loops.
NIS2-21-4	The organisation shall assess supplier and third-party security practices.	A, R	FA-02, FA-05, FA-08	Partially Covered	Supply chain risks are identified and treated, but third-party audit procedures require explicit extension in the Risk Management Plan.
CRA-13-15	The manufacturer shall provide compliance documentation to authorities upon request.	R	FA-05, FA-08	Conditionally Covered via R	Document availability is governed by the structure and scope of the Risk Management Plan, but is not enforced by default.

4.3. FAST Mapping and Compliance Assessment

Each acceptance criterion was mapped to one or more FAST components and artefacts to determine whether outputs from FAST can serve as evidence of compliance. Coverage was evaluated using four categories: *Fully Covered*, *Partially Covered*, *Conditionally Covered via R*, and *Not Covered*. The conditional category refers to obligations met only when explicitly managed through the Risk Management Plan (R).

Table 4 summarises the coverage distribution. CRA shows stronger alignment with FAST, while NIS2 more often requires extensions to risk-management activities.

Table 4
Coverage distribution of NIS2 and CRA obligations by FAST

Coverage Level	NIS2 (%)	CRA (%)
Fully Covered	10.0	21.9
Partially Covered	10.0	3.1
Conditionally Covered	60.0	61.5
Not Covered	20.0	13.5

These results indicate that while FAST offers strong structural support for security analysis and mitigation, complete compliance with NIS2 and CRA also depends on broader governance and lifecycle processes within risk management, such as treatment planning and continuous monitoring.

5. Evaluation: Expert Feedback

To validate the requirement extraction and assess the practical value of FAST in supporting compliance, expert feedback was gathered from five professionals with backgrounds in security law, product security, and public sector governance.

5.1. Procedure and Participants

The objective of the validation was twofold: (1) to verify the correctness and completeness of the extracted NIS2 and CRA obligations and their mapping to FAST, and (2) to assess FAST's usefulness as a compliance support framework in practice. Experts were sought who could represent legal, technical, and organisational viewpoints. Twenty professionals with relevant backgrounds across academia, industry, and the public sector were contacted; five agreed to participate. The expert group represented both private and public organisations, as well as diverse roles (Table 5).

The validation followed two stages. First, participants received the compliance artefact containing extracted requirements, classification schema, mapped FAST artefacts, and acceptance criteria. Second, semi-structured interviews were conducted to discuss their feedback, with several participants also providing written comments.

Table 5
Expert Participants in Compliance Artefact Validation

Expert ID	Role and Affiliation
Expert 1	Legal Advisor, Telecommunication Company
Expert 2	Product Manager, Device Security Solutions, Legal Consultancy Company
Expert 3	Legal Analyst and Intellectual Property Officer, R&D Company
Expert 4	Legal Analyst, R&D Company
Expert 5	Cybersecurity Technology Advisor, Governmental Institution

5.2. Insights from Validation

Experts found the artefact well structured and traceable: each requirement could be linked to its legal origin, mapped FAST element, and acceptance criterion. They noted that the explicit reasoning behind mappings improved credibility and practical usability.

Interviews highlighted differences in regulatory scope. NIS2, as a directive, depends on national transposition, while CRA applies directly across the EU. This creates compliance overlap—some obligations are immediate under CRA, others arise indirectly through NIS2 implementation. Despite this, experts agreed both laws are risk-based: NIS2 focuses on organisational resilience and governance, CRA on product design, vulnerability handling, and lifecycle management.

Experts outlined several approaches for meeting these requirements:

- Identify critical business processes and related assets, then conduct risk analysis based on dependencies and threat exposure.
- Follow structured frameworks such as ISO/IEC 27001 or Estonia's E-ITS standards for auditable compliance.

- Perform compliance gap analyses to locate and prioritise control deficiencies.

Some suggested grouping obligations by domain rather than article for easier use. Others pointed to supporting materials such as RIA's sectoral risk analysis templates [30] and ENISA's implementation guides [31] as useful complements.

Experts viewed FAST as a practical, integrative method linking functional and asset-based risk assessments. Its risk-driven treatment logic enables organisations to tailor controls to obligation-specific needs, supporting both compliance and operational assurance. For SMEs, FAST was seen as a clear entry point to handle regulatory complexity by embedding security and compliance into existing processes rather than adding new layers. Several participants proposed developing a concise, role-based guide to further assist adoption—identified as a promising avenue for future work.

5.3. Resulting Adjustments and Reflections

Expert feedback led to refinements improving clarity and traceability:

- Acceptance criteria were revised to align more closely with regulatory language.
- Role definitions, particularly for notified bodies and economic operators, were clarified.

The validation mainly examined the regulatory mappings and resulting artefacts, not FAST's internal structure. Future studies should extend evaluation to operational scenarios such as audit planning and system design. Nonetheless, the feedback confirmed FAST's relevance as a risk-aware foundation for managing security obligations under NIS2 and CRA.

6. Concluding Remarks and Future Work

This paper presented a structured alignment of the FAST security framework with obligations in the NIS2 Directive and the Cyber Resilience Act (CRA). We extracted and classified applicable requirements, formulated traceable acceptance criteria, and mapped them to actionable FAST components. Expert review confirmed traceability, legal alignment, and practical utility for compliance planning.

A key outcome is that FAST's risk-based logic aligns with core compliance principles in both NIS2 and CRA. By embedding obligation fulfilment within function- and asset-level risk analysis, FAST enables organisations—particularly SMEs—to approach compliance through structured decision-making rather than reactive checklists. Experts noted that this helps reconcile organisational obligations under NIS2 with product-focused requirements under CRA, offering a unified analytical lens.

The validation served its intended purpose: to assess whether FAST can meaningfully support compliance under current regulatory expectations. The evaluation focused on manufacturers to manage complexity; other roles (e.g., service providers, importers) were not included. The broader legal context—especially differences between directives and directly applicable regulations—remains a challenge for generalisation and automation. FAST does not remove this complexity but provides a systematic way to navigate it.

Future work should: (i) deploy FAST in real industrial settings to test operational usability, including audit planning and risk treatment justification; (ii) expand scope to additional roles and cross-sectoral dependencies; and (iii) develop a concise, role-based or function-oriented compliance guide for SMEs, as suggested by experts.

Overall, this research contributes to bridging evolving regulatory obligations and operational security practice. As industrial systems become increasingly interconnected and regulated, structured methods like FAST can serve as a framework for embedding compliance into core engineering and governance workflows.

Acknowledgments

The European Union funds this research under Grant Agreement No. 101087529. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible.

Declaration on Generative AI

The authors declare that generative AI tools were used solely for language editing and style improvement. Specifically, ChatGPT (OpenAI GPT-5, 2025) and Grammarly were employed to enhance readability, grammar, and clarity of the text. No generative AI tools were used for data generation, analysis, interpretation, or the formulation of research content. The authors take full responsibility for the accuracy, originality, and integrity of all scientific content presented in this paper.

References

[1] European Commission. Directorate General for Energy., ECORYS., The net-zero manufacturing industry landscape across Member States: final report., Publications Office, LU, 2025. URL: https://data.europa.eu/doi/10.2833/2249632.

[2] European Union Agency for Cybersecurity., ENISA threat landscape 2024: July 2023 to June 2024., Publications Office, LU, 2024. URL: https://data.europa.eu/doi/10.2824/0710888.

[3] E. A. Lee, Cyber physical systems: Design challenges, in: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008, pp. 363–369. doi:10.1109/ISORC.2008.25.

[4] A. Ocaka, D. O. Briain, S. Davy, K. Barrett, Cybersecurity threats, vulnerabilities, mitigation measures in industrial control and automation systems: A technical review, in: 2022 Cyber Research Conference - Ireland (Cyber-RCI), 2022, pp. 1–8. doi:10.1109/Cyber-RCI55324.2022.10032665.

[5] G. Murray, M. N. Johnstone, C. Valli, The convergence of it and ot in critical infrastructure, in: Proceedings of the 15th Australian Information Security Management Conference, 2017, pp. 149–155. URL: https://ro.ecu.edu.au/ism/217/. doi:10.4225/75/5a84f7b595b4e.

[6] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, M. Kantarcioglu, Security and privacy in cyber-physical systems: A survey of surveys, IEEE Design Test 34 (2017) 7–17. doi:10.1109/MDAT.2017.2709310.

[7] European Union, Directive (EU) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union (NIS2 Directive), 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555, accessed: 2025-01-23.

[8] European Union, Regulation (EU) 2024/2847 of the european parliament and of the council of 12 december 2024 on measures for a high common level of cybersecurity for products with digital elements (Cyber Resilience Act), 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847, accessed: 2025-01-23.

[9] N. Vandezande, Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor, Computer Law & Security Review 52 (2024) 105890. URL: https://linkinghub.elsevier.com/retrieve/pii/S0267364923001000. doi:10.1016/j.clsr.2023.105890.

[10] P. Eckhardt, A. Kotovskaia, The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive, International Cybersecurity Law Review 4 (2023) 147–164. URL: https://link.springer.com/10.1365/s43439-023-00084-z. doi:10.1365/s43439-023-00084-z.

[11] A. van Welie, Legislation within cybersecurity: preparing for NIS2 – a detailed framework in the healthcare sector in the Netherlands, Master's thesis, Cybersecurity/Turku School of Economics (TSE) & Tilburg School of Economics and Management (TiSEM), 2024.

[12] Z. S. Li, C. Werner, N. Ernst, D. Damian, Towards privacy compliance: A design science study in a small organization, Information and Software Technology 146 (2022) 106868. URL: https://linkinghub.elsevier.com/retrieve/pii/S0950584922000362. doi:10.1016/j.infsof.2022.106868.

[13] K. A. Parvanov, From Legislation To Practice A Structured Guide for the EU's Cyber Resilience Act, Master Degree Project, University of Skövde, 2024.

[14] V. Antipenko, R. Matulevičius, Functional security in automation: The fast approach, in: E. Paja, J. Zdravkovic, E. Kavakli, J. Stirna (Eds.), The Practice of Enterprise Modeling, Springer Nature Switzerland, Cham, 2025, pp. 244–261.

[15] M. Veigurs, T. Lasmanis, A. Romanovs, IT Governance in Critical Sectors: Towards the NIS2 Implementation, in: 2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), IEEE, Riga, Latvia, 2024, pp. 1–7. URL: https://ieeexplore.ieee.org/document/10741938/. doi:10.1109/ITMS64072.2024.10741938.

[16] A. J. Jara, I. C. Martinez, J. S. Sanchez, CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2, in: 2024 IEEE Smart Cities Futures Summit (SCFC), IEEE, Marrakech, Morocco, 2024, pp. 56–60. URL: https://ieeexplore.ieee.org/document/10698057/. doi:10.1109/SCFC62024.2024.10698057.

[17] D. Skias, S. Tsekeridou, T. Zahariadis, A. Voulkidis, T.-H. Velivassaki, Demonstration of alignment of the Pan-European Cybersecurity Incidents Information Sharing Platform to Cybersecurity policy, regulatory and legislative advancements, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ACM, Vienna Austria, 2022, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3538969.3544477. doi:10.1145/

3538969.3544477.

[18] Yogosha, Cyber resilience act: A comprehensive guide to compliance and implementation, n.d. URL: https://yogosha.com/blog/cra-cyber-resilience-act-guide/, accessed: 2025-01-23.

[19] V. Antipenko, R. Matulevičius, Function–threat alignment in cps with fast and mitre att&ck, in: R. Deneckère, M. Kirikova, J. Grabis (Eds.), Perspectives in Business Informatics Research, Springer Nature Switzerland, Cham, 2026, pp. 365–379.

[20] S. Alter, The Work System Method: Connecting People, Processes, and IT for Business Results, Work System Method, 2006.

[21] É. Dubois, P. Heymans, N. Mayer, R. Matulevičius, A Systematic Approach to Define the Domain of Information System Security Risk Management, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 289–306. URL: https://doi.org/10.1007/978-3-642-12544-7_16. doi:10.1007/978-3-642-12544-7_16.

[22] R. Matulevičius, Fundamentals of secure system modelling, Springer, 2017.

[23] A. Shostack, Threat Modeling: Designing for Security, John Wiley & Sons, 2014.

[24] MITRE, Mitre att&ck for ics (industrial control systems), n.d. URL: https://attack.mitre.org/matrices/ics/, accessed: 2025-01-23.

[25] T. Breaux, A. Antón, Analyzing regulatory rules for privacy and security requirements, IEEE Transactions on Software Engineering 34 (2008) 5–20. doi:10.1109/TSE.2007.70746.

[26] J. F. Zarrabi, H. Mouratidis, S. Islam, Extracting security requirements from relevant laws and regulations, IEEE, 2012.

[27] K. Fatema, C. Debruyne, D. Lewis, D. OSullivan, J. P. Morrison, A.-A. Mazed, A semi-automated methodology for extracting access control rules from the european data protection directive, in: 2016 IEEE Security and Privacy Workshops (SPW), IEEE, 2016, pp. 25–32.

[28] S. Islam, H. Mouratidis, S. Wagner, Towards a framework to elicit and manage security and privacy requirements from laws and regulations, in: R. Wieringa, A. Persson (Eds.), Requirements Engineering: Foundation for Software Quality, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 255–261.

[29] D. Firesmith, Engineering Safety and Security Related Requirements for Software Intensive Systems., in: ICSE Companion, 2007, p. 169.

[30] Estonian Information System Authority, Cybersecurity Assessment and Roadmap Methodology (v2), Deliverable D2.1, Estonian National Cybersecurity Centre (NCC-EE), 2024. URL: https://www.ria.ee/sites/default/files/documents/2024-09/NCCEE-WP2-D2.1-Cybersecurity-Assessment-and-Roadmap-Methodology_v2.pdf, accessed: 2025-06-13.

[31] European Union Agency for Cybersecurity (ENISA), Implementation Guidance on Security Measures: For Public Consultation, Technical Report, ENISA, 2024. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation%20guidance%20on%20security%20measures_FOR%20PUBLIC%20CONSULTATION.pdf, accessed: 2025-06-13.