Critical Infrastructure Risk Assessment: Current Practices and Emerging Challenges

Lennart Kiss, Sirish Kalubhai Savaliya[1], Christian H. Schunck, Rachelle Sellung, Matthias Winterstetter[2]

Abstract: Operators of critical infrastructures face a rapidly evolving, hybrid threat landscape under tight budgetary and staffing constraints. This paper focuses on the prerequisite for effective defense— "you cannot protect what you do not know"—and the practical difficulty of mapping threats to both internal assets and supplier networks to prioritize mitigation. We combine a state-of-the-art review of asset/configuration and risk management with an exploratory mixed-methods study: 11 semi-structured interviews with IT security and procurement stakeholders from large European CI operators (e.g., international airports). Using a hybrid coding approach in MAXQDA and thematic analysis, we surface organizational, technical, and governance challenges across IT/OT and deep-tier supply chains. We synthesize requirements and propose [Project Name], a BMBF-funded demonstrator that integrates automated asset discovery, supplier intelligence, and risk-value scoring to generate prioritized, evidence-based mitigation actions aligned to resource constraints and support more trustworthy, auditable risk decisions in digitally connected CI ecosystems.

Keywords: Critical Infrastructures, Risk Assessment, Supplier Management, Stakeholder Research, Risk Value Scoring, Crisis Management

1 Introduction

Critical infrastructures (CI) operate in an environment where cyber, physical, and informational threats increasingly blend into hybrid campaigns, stress-tested by geopolitical and environmental shocks [Ol25]. At the same time, CI operators must make defensible risk decisions with limited budget and personnel. While the maxim "you cannot protect what you do not know" is widely accepted, two knowledge problems persist in practice: (1) incomplete, aging knowledge about in-scope assets and configurations across IT and OT; and (2) limited, shallow visibility into supplier

[1] University of Stuttgart IAT, Identity Management, Allmandring 35, Stuttgart, 70569, lennart.kiss@iat.uni-stuttgart.de https://orcid.org/0009-0000-8839-5470, sirish-kalubhai.savaliya@iat.uni-stuttgart.de https://orcid.org/0009-0001-3951-3482
[2] Fraunhofer IAO, Identity Management, Nobelstrasse 12, Stuttgart, 70569, christian.schunck@iao.fraunhofer.de https://orcid.org/0000-0002-6065-6226, rachelle.sellung@iao.fraunhofer.de https://orcid.org/0000-0003-1235-030X2, matthias.winterstetter@iao.fraunhofer.de https://orcid.org/0000-0001-9093-4381

doi:10.18420/OID2026_05

networks where vulnerabilities and compromises can propagate as cascading risks. Without trustworthy asset and supplier intelligence, mapping threats to impact remains ad hoc, and mitigation efforts are hard to prioritize.

The first knowledge problem has intensified as OT environments become digital and connected. Asset and configuration management has moved from best practice to necessity, yet CI realities complicate execution: legacy and safety-critical systems may not tolerate scanning; inventories drift rapidly; and integrating heterogeneous sources into a single source of truth is non-trivial. Automation is essential but "scan or not to scan" remains a live trade-off in mixed IT/OT networks. Standards and guidance, including CISA's OT asset management work, ISO/IEC 62443 [Se26], and NIST SP 800-82 [St23], underscore this criticality, but operationalization in CI is uneven.

The second knowledge problem concerns suppliers. CI resilience depends on vendors, integrators, and deep-tier sub-suppliers that are often opaque, globally distributed, and heterogeneous. Regulatory and institutional responses are advancing—NIST SP 800-161 [Bo22], CISA's push for SBOM transparency [CI26], and NIS-2 [Bu25] —yet guidance remains fragmented across sectors and jurisdictions, and enforcement asymmetries persist. Commonly used supplier evaluation approaches include MCDM methods (e.g., AHP, TOPSIS, VIKOR, DEMATEL) [El21] and data-driven/ML techniques [Si23]. These help structure decisions but suffer from subjective weighting [Ku03], limited interpretability, and uneven data availability across CI sectors—especially where real-time telemetry is scarce or regulated [Si23]. Deep-tier visibility remains weak [BS24], governance is siloed across IT, OT, and procurement [CCM19], and human decision biases are under-addressed in risk processes [PDB24]. Meanwhile, the field has shifted from guaranteeing absolute protection to engineering systemic resilience—anticipate, withstand, recover, and adapt with methods emphasizing explicit treatment of threat, vulnerability, and consequence [Bo22].

Against this backdrop, our work asks how CI operators can turn asset and supplier knowledge into actionable, prioritized mitigation under resource constraints. We structure the paper around three research questions: RQ1: What practical obstacles hinder establishing and maintaining trustworthy asset and configuration knowledge across IT/OT in CI organizations? RQ2: What are the key challenges in supplier risk management for CI, including deep-tier visibility, assurance, and governance? RQ3: How can asset and supplier intelligence be operationalized into risk-mitigation and workflows that prioritize actions suited to limited budget and personnel?

To address these research questions, we conducted a mixed-methods study and summarized the findings in the following chapters. Chapter 2 provides an overview of related work and literature from research. Chapter three consists of a structured review of the current state of the art in asset/configuration management and risk assessment in CI. Chapter four presents an exploratory, mixed-methods empirical research of experts working with supplier management in CI. After presenting the summaries of both desk and empirical research, a discussion (chapter five). This includes an overview of the

research questions and a demonstrator idea that operationalizes these findings.

2 Related Work

This section expands on the research that has been done on Key Challenges and Gaps in CI Supplier Risk Management. It will present the persistent challenges hindering effective Risk Management and Assessment. Covering both high-level structural challenges as well as institutional guidance on the matter. The methods and strategies surrounding Critical Infrastructure Protection (CIP) have fundamentally shifted from a narrow focus on protection of individual assets against threats toward a holistic emphasis on systemic resilience. This is mainly due to the increasing interconnectivity of modern infrastructures. As assets grow in volume and complexity, maintaining absolute protection within a networked environment has become both technically and economically unfeasible. Thus, raising the necessity of methodologies that prioritize the ability of systems to anticipate, withstand, recover from and adapt to adverse events [Bo22]. Accordingly, robust business continuity and rapid restoration capabilities also gained importance.

Despite the theoretical convergence on the goal of resilience, institutional guidance efforts take unique approaches in their enforcement mechanisms and strategic focus, creating a regulatory basis with certain differences between them. The National Institute of Standards and Technologies (NIST) continues to provide the foundational architecture for risk management through their SP 800-161 document. Within this guidance, voluntary yet rigorous standards for supply chain risk management practices are outlined [Bo22]. In contrast, the approach of the Cybersecurity and Infrastructure Agency (CISA) focusses heavy on transparency, showcased by their efforts to push adoption of Software Bill of Materials (SBOM) initiatives, that ultimately aim to shine light on the opacity of software supply chains [CI26]. All the while, the German Federal Office for Information Security (BSI) transitioned to a strict mandate-led environment. Their IT Security Act 2.0 exemplifies this, by imposing significant legal penalties for non-compliance and demanding declarations of trustworthiness for critical components [Fe21].

While executing a task of described complexity and scale, one can find a field of challenges and barriers in the CI ecosystem. For one, the practical application of these risk assessment methodologies places a disproportionate burden on Small and Medium-sized Enterprises (SMEs) due to shortage of dedicated cybersecurity expertise and financial constraints. These companies are often deeply intertwined in the supply chain system and therefore directly impacting the CI's security [JK25]. However, factors that impact all sizes of Enterprises can be found by looking into governance and organizational cultures. Internal control systems and employee attitudes are one of the most salient predictors of cyber resilience, yet many organizations report to be suffering under leadership deficiencies and inconsistent policy enforcement rendering technical controls less impactful [Fr25]. This is compounded by existing data scarcity and

knowledge gaps. Consequently, methods often fail to adequately address uncertainty and instead rely on “worst reasonable case” assumptions [Wh16].
Specific to the domain of Supplier Risk Management, several challenges and gaps remain. First, a lack of standardized taxonomy, such as inconsistent definitions of the “supply chain” and fragmented Cyber Supply Chain Risk Management (C-SCRM) guidance across different sectors and regions impede the development of unified risk language [To21]. Supplier Risk Management processes tend to achieve poor mapping beyond Tier-1 suppliers, leaving those further along the chain as critical blind spots [BS24]. This is further worsened by the involvement of different stakeholders and their interdepartmental dynamics. Organizational silos and the disconnect between stakeholders, such as IT, OT and procurement as well as legal departments to some extent result in limited centralized governance over C-SCRM processes [CCM18]. However, the problem may not just be resolved by centralized governance and knowledge sharing processes of extensive databases without considering the human factor. Risk assessment processes often fail to account for human biases and socio-technical complexity in managing multi-stakeholder systems [PDB24]. Most importantly, current practices remain predominately reactive and incident-driven, accompanied by lacking continuity planning with suppliers in mind, rather than proactive collaboration required to secure modern critical supply chains [PDB24].

3 State of the Art

This section summarizes state-of-the-art practices in (1) asset and configuration management, (2) supplier management, and (3) risk management in critical infrastructure contexts.

3.1 Asset- and Configuration-Management

The topic of Asset- and Configuration-Management for IT (Information Technology)- and OT (Operation Technology)-Assets and Configuration Items has been getting increasingly more attention in recent years, from both the governmental and academic position. This interest also extends to critical infrastructure in this area [WDG23]. As OT environments become increasingly digital and connected, maintaining accurate IT/OT asset and configuration knowledge has become a prerequisite for security (“you can only protect what you know”) [Ve25, AL24]. Because modern IT/OT networks contain large numbers of heterogeneous devices, automated discovery and inventory updates are essential [GKS05]. Common approaches are (1) active scanning, (2) passive monitoring, and (3) endpoint agents.
There are several unresolved challenges in the field of asset and configuration management that are particularly pronounced in environments involving critical infrastructure and operational technology (OT). While asset management is a well-

established discipline, the increasing complexity and heterogeneity of modern OT environments continue to expose fundamental limitations in current approaches. A central objective of asset management is the identification and continuous maintenance of accurate information about all assets within an environment. As systems grow in size and complexity, however, achieving a complete and up-to-date overview becomes increasingly difficult. In highly complex infrastructures, this challenge often leads organizations to operate with asset inventories that are known to be incomplete. Such partial visibility is frequently accepted as an operational reality; despite the risks it poses. This is largely due to the operational reality that a passive scan cannot find devices that don't talk while active scans might not be usable due to the sensitivity of some devices in the Network. A Discussion around these challenges can be found in [Sa22], where they are discussed in more detail. Another concern regarding scanning tools is the sensitivity of OT Networks towards high traffic and unexpected communication protocols. While passive scanning can still be used without issue in these environments, active scanning can pose significant risks which can lead to a shutdown of the scanned devices This issue is discussed in [Ed19] and [Sa22] with more detail.

Asset and configuration management systems are typically intended to function as a single source of truth that supports and informs other management and security processes. Achieving this role in practice is particularly challenging in critical infrastructure environments, which are often characterized by a high degree of heterogeneity and the continued use of legacy systems and databases. As mentioned in [Al20] this is even a challenge in IT Systems which are, due to their nature of not containing OT devices, less heterogeneous in most cases. Finally, organizations face the challenge of selecting appropriate tools from a highly fragmented and saturated market. Asset discovery and inventory management can be approached using a wide range of techniques, and these are implemented by a large and growing number of vendors. At the time of writing, publicly available tool listings identify several hundred solutions addressing asset discovery alone, as can be seen in [Cy26]. This abundance of tools, many of which offer overlapping functionality, complicates decision-making and increases the risk of tool sprawl, integration difficulties, and inconsistent data quality, particularly in complex OT environments. Although some efforts have already been made to ease the process of finding an appropriate tool in [Sa22] by creating a taxonomy for scanning tools, the topic of asset and configuration management is larger than just scanning and requires more attention from the research community.

3.2 Supplier Management Systems

Effective supply chain management is essential for company strength and operational excellence [El21]. A key component of this process is supplier evaluation, which entails carefully assessing suppliers to make sure they meet an organization's requirements for cost, performance, execution, and sustainability [KD25]. Well-drafted supplier evaluation process makes it possible for Critical Infrastructures or Organizations to overcome the operational risks, improve performance and transparent supplier

relationships [Go23]. However, this process has become increasingly difficult due to globalization, developments in digital technologies, and the growing emphasis on sustainability. To manage the complexity of supplier evaluation processes, organizations highly depend on various theoretical frameworks practice [DM03]. Among these, multi-criteria decision-making (MCDM) frameworks are widely adopted, it allows organizations to evaluate supplier based on multiple, often conflicting criteria like cost, quality, performance, risk and sustainability [HXD10]. The common techniques of MCDM include Technique for Order preference by Similarity to ideal Solution (TOPSIS), Analytic Hierarchy Process, VIKOR, and DEMATEL [El21]. These methods help decision makers rate weights to criteria and compare competitive alternative suppliers in transparent and structured manner [Go15]. However, MCDM-based process has challenges like subjective weighting, interdependent criteria, method selection, which can lead to inaccurate or biased rankings. Lake of standardization and slight variations further reduce the reliability and robustness of the results [Ku03].

Another technique in current supplier evaluation is Advance Data-Driven & Machine Learning techniques have emerged within Industry 4.0 environment. By using massive historical dataset and real-time data from IoT/OT systems, organizations perform big data analytics to forecast supplier performance, identify potential risks, and predict supplier failures [OOE25, Si23]. This method not only enhances efficiency, predictive analytics, and risk management but also helps firms pick and prioritize suppliers based on objectively evaluated operational data [Cu22]. However, this kind of approach is mostly limited to data-rich environments. For most other suppliers, acquiring correct and full data is extremely challenging due to availability, compliance, confidentiality, and reporting issues, which affects model reliability and makes implementation problematic [Si23]. Additionally, issues such as biased historical data, limited interpretability, and feature selection challenges may affect evaluation accuracy [Mo23]. Overall, the existing supplier management approaches relieve MCDM-based framework and advance data-driven approaches. While both of them provide valuable decision support but also showing challenges in terms of subjectivity, data dependency, and scalability, limiting their ability to deliver universally robust and standardized assessments across critical infrastructure sectors.

3.3 Risk Management

With effective asset and supply chain management in place, an organization has a strong foundation for security-related decision making, including risk management. Importantly, the decisions that follow from risk assessments are usually not made by specialists with deep security expertise capable of rapidly interpreting technical risk output. Instead, these decisions must be made by managerial stakeholders with backgrounds in economics or finance who have to quickly understand the problem at hand and make well-founded, informed decisions. From a governance perspective, this gap in domain expertise at the decision-making level presents a significant challenge: security risks must be translated into information that management can readily interpret

and act upon. Research indicates that while sophisticated risk measurement instruments and cybersecurity tools are developing, there remains limited information and metrics presented in a language that non-technical decision makers, such as Boards of Directors or executives, can easily understand and use for governance purposes as discussed in [MKG23]. In practice, approaches such as qualitative risk matrices, semi-quantitative scoring models, and key risk indicators are used to support decisions, but these frequently fail to connect technical risk values with business impact in a way that is intuitive for managers and executives [MKG23, PKS23]. A core challenge of the risk management process is therefore not only generating accurate risk assessments but enabling decision making by stakeholders without a security background. A potential avenue for research in this area involves developing value and risk representations that explicitly relate an asset's business or economic value to its risk exposure, thereby making security information more readily understandable and actionable for managerial decision makers.

4 Empirical Study on Supplier Management in CI's

The following chapter presents the methodology and research results of the explorative empirical study conducted with critical infrastructure experts working with supplier management.

4.1 Methodology

The study followed a mixed methodology approach, which focused on qualitative interviews with the support of a short questionnaire. The qualitative interviews followed a semi-structured approach. It included a multi-stakeholder sample of 11 interview participants. The sample represented experts working in various departments (e.g. IT Security, Procurement) and roles (e.g. Team Leads, Team Members) in the critical infrastructure sector (e.g. International Airports) in central Europe. There were four different critical infrastructure operators that participated in the study. The scope of the study focused on gaining insights on how risk assessment is conducted for supplier management of a critical infrastructure. Therefore, participants needed to be experts with demonstrated experience with these use cases.

Regarding data collection and preparation, there were three parts to the semi-structured interview questionnaire. The first part inquired about the current standards and processes for supplier management; in particular, new supplier evaluation and current supplier monitoring and auditing. The second section dove deeper into challenges and risks and potential improvement. In the final section, the participants were asked about a technical solution that could support their fore-mentioned processes and the requirements and needs they would have. Overall, each interview ranged about 45 minutes to one hour in length. After each interview was conducted, the data was it was transcribed and coded

using MAXQDA program. In order to conduct a Thematic Analysis [BC23], a hybrid coding approach with both an inductive and deductive was used. The coding catalog has been based on the exploratory research questions. The main goal is to understand existing processes and structures of supplier management; pain points and potential; and technological solution questions of their needs and preferences. The catalog went through two iterations. The first iteration included an expert analysis where a base coding set was first established using the themes of the semi structured interview questionnaire. After the interviews were coded independently by multiple experts, a workshop was held to discuss the second iteration of the coding system. Aside of aligning the definitions of each code, the key revisions made were to orient according to use case, introduction of "roles and responsibilities" branch, and the expansion of risks and challenges. The enabled a consistent and structured approach to identifying patterns and themes across the data.

4.2 Qualitative Results

This section describes the results on existing risks and challenges in critical infrastructures. There are three main themes identified for the challenges; 1.) Supplier, 2.) Technical and Security and 3.) Structural and Organizational. Quotes from participants will be described with their respective numbers P1-11.

Supplier Challenges

First, the communication and transparency on either incidents or internal changes don't always seem to align with the expectations of the participants. For example; one participant expressed *"And of course, I want to be informed early on so that we can discuss how to handle the handover or how this can be done. Of course, this happens very, very rarely. Most of the time, we find out 2-3 days in advance that an employee is leaving the company." (P8, 2025)* Second, participants spoke often of constraints regarding support from the supplier for different tasks, while most support would come as a reaction instead of being proactive about security incidents or requirements. In addition, all four critical infrastructure operators relied on the supplier to report any security incidents and their own self attestation. When asked about this in detail, participants elaborated on their thoughts of lack of transparency of security mechanisms or their fears of delay of response in security incidents.

Technical and Security and related Challenges

Participants spoke out about a variety of technical and security related issues. Regarding security maintenance and configuration, some gave examples of their concerns of suppliers neglect of fundamental practices like using multi-factor authentication, system updates, or patch management. Some interviewees voiced that they felt that suppliers did not prioritize security related requirements. In addition, experts elaborated on their point of view that there is an insecurity about patch management from vendors and fears regarding outdated frameworks or poorly maintained configurations. *"So what I'm*

noticing is that there's a massive lag between what you actually need to have and what many service providers have. That means that due to a lack of prioritization, be it due to a lack of resources, I keep noticing that simple things like multi-factor authentication, for example, are not activated. …" (P1, 2025) In addition, one participant observed that small suppliers sometimes lack security competency or experience. *"So, especially in the OT world, where there are many small suppliers who don't have much in the way of security... they have very good functional solutions, but not yet security solutions, i.e., secure solutions, and securing them and also driving their mindset in that direction so that they really develop security awareness and not just functional requirements... I think that's definitely a big challenge. Especially in the OT world." (P9, 2025)*

Organizational and Structural Challenges

Considering the Organizational and Structural issues, the following situations were described by experts. First, there appears to be a lack of effective penalty mechanisms, where even if there is a contract clause for bad performance or security practices, it seems like that they were not often enforced. In addition, some participants describe the difficulty of terminating suppliers that are critical to operation, even in extreme situations (e.g. severe security issues). Second, some touched on how the evaluation of suppliers from internal department is sometimes incomplete or incorrect, which lead to misclassifying the supplier criticality. This can lead to not having the necessary security measures in place or delayed. Third, it was often discussed how cyber incidents are often reported late or not at all and how this becomes a downstream risk. *"First, there is the risk that it will occur, then the risk that we will notice it too late, because perhaps the supplier has not provided satisfactory information about it. The same applies, incidentally, to security issues and the compromise of the supplier. Of course, there is also the downstream risk that the supplier is not really well informed or that we do not recognize it well."(P2, 2025)* Lastly, most of the critical infrastructures that participated in the study largely relied on the self-assessment of suppliers; however, this can lead to challenges of lack of validation of self-proclaimed security compliance. *"Well, what we see most often is that they write down all the great things they can do on paper, but then they fail to deliver."* (P3*, 2025*)

5 Discussion

After considering the related work, current state of the art, and empirical results on risk assessments in critical infrastructures, this section discusses the research questions stated in the introduction and presents a demonstrator project that aims to address some of the challenges summarized in this work.

5.1 Research Questions

This study sets out to address the critical gap between the theoretical necessity of

comprehensive risk assessment and the practical realities faced by CI operators. By putting a thematic review of current state-of-the-art practices and related work highlighting existing challenges head-to-head against a semi-structured interview with 11 CI stakeholders, we addressed three research questions: (RQ1) What practical obstacles hinder establishing and maintaining trustworthy asset and configuration knowledge across IT/OT in CI organizations? (RQ2) What are the key challenges in supplier risk management for CI, including deep-tier visibility, assurance, and governance? (RQ3) How can asset and supplier intelligence be operationalized into risk-mitigation and workflows that prioritize actions suited to limited budget and personnel? The following sections detail the findings, comparing the thematic baseline with the empirical evidence gathered during our qualitative analysis.

In addressing RQ1, our findings emphasize that establishing trustworthy asset knowledge is hindered by both technical and organizational factors. Literature underscores the technical risk that active scanning poses to legacy and safety-critical systems. Our qualitative research confirms these concerns and identifies more specific operational hurdles. Participants noted that active scanning is often avoided because it can cause errors in sensitive operational technology (OT) environments. Furthermore, our research identified a significant challenge in the complexity of managing asset information requirements from various stakeholders. Different departments have distinct data needs, which makes it difficult to maintain a consistent inventory. Operators must also contend with the integration of legacy database systems that were not designed for modern automated discovery. These factors contribute to the persistence of incomplete inventories across the sector.

Regarding RQ2, our study first confirms several key challenge themes identified in the existing literature. These include the inherent lack of transparency in deep-tier supply chains and the burden created by fragmented regulatory requirements. Our qualitative interviews verify that visibility into sub-suppliers remains a significant hurdle for CI operators. However, it was uncovered that specific governance failures that are less emphasized in current academic discourse. A primary contribution of our research is the identification of a "dependency trap." Our data shows that CI operators often experience a severe power asymmetry when dealing with global vendors. Even when security deficiencies are known, operators feel unable to terminate contracts due to a total reliance on specific software or hardware ecosystems. Furthermore, we found that contractual penalty mechanisms, such as malus clauses, are rarely enforced in practice. Operators may choose to play down these security-related breaches to avoid straining relationships with essential providers. These findings suggest that the challenge is not a lack of legal frameworks but rather the market dynamics that favor large-scale suppliers over individual infrastructure operators.

Finally, our findings for RQ3 suggest a positive path forward for managing these risks under resource constraints. While literature frequently focuses on the general shortage of cybersecurity experts, our research identified "internal sources of error" as a more specific bottleneck. For example, non-security departments often provide inaccurate

criticality data during the onboarding process. This suggests that the solution to effective prioritization lies in the integration of business intelligence with technical discovery. We found a significant need for systems that can automatically validate internal data against real-world asset configurations. This poses an opportunity for the implementation of automated systems that can synthesize asset discovery, supplier intelligence, and risk-value scoring. Taken together, the findings for RQ1–RQ3 indicate a need for a practical mechanism that combines asset visibility, supplier intelligence, and resource-aware prioritization. The following demonstrator is proposed as that operational response.

5.2 Demonstrator Project

The results of these studies show that asset management and supplier evaluation require significant overhead. On the other hand, these are key to distinguish in a large threat landscape those threats that can lead to large scale interruption of operations for CIs. The identification of these threats and prioritizing mitigation actions must be automatized to the largest extent possible to cope with limit budgets and personnel resources.

The demonstrator project "AEROKI" [Bu23] has worked with CIs to deliver strategies and explore solutions for semi-automatic asset management, continuous supplier monitoring, as well as semi-automatic identification of relevant threats and mitigations. For the last point we propose going beyond a mere risk analysis but comparing the business value delivered by IT/OT systems in relation to their quantified risk exposure, yielding a transparent risk-value score that drives prioritization and concrete response under real-world constraints. Within the demonstrator project, risk-value scoring links two dimensions: a dynamic risk score that reflects threat likelihood and potential impact (based on vulnerability severity, exploit availability, exposure, supplier posture, patch status, and compensating controls), and a business value score that captures the criticality of the affected service and its contribution to business impact and value creation. By continuously ingesting signals from asset inventories, SBOMs, vulnerability and patch management, supplier evaluations, and threat intelligence, the platform updates both dimensions and computes a normalized risk-to-value assessment per system and dependency chain. Decision thresholds translate this assessment into action: when risk exceeds value and patching is infeasible, the system recommends temporary isolation or shutdown; when value is high and risk is moderate, it prioritizes compensating controls such as segmentation, rate limiting, virtual patching, or accelerated supplier remediation; when both risk and value are high, it escalates to executive risk acceptance with documented time-boxed mitigations. The scoring and its inputs are made fully transparent through security KPIs and audit trails to support defensible, repeatable decisions in special situations (e.g., Log4Shell-class vulnerabilities).

This approach does not replace architectural hardening; however, it provides immediately actionable, semi-automated prioritization that complements a Zero Trust roadmap. In the short term, risk-value scoring enables rapid, budget-aware triage and targeted mitigations; in the medium term, it informs which systems and suppliers should

be migrated first to Zero Trust controls based on the greatest risk-reduction per unit of business value preserved. The demonstrator project should validate the method in a realistic CI environment and deliver operational playbooks, threshold policies, and a reference implementation that organizations can sustain in the future.

6 Conclusion

Addressing the challenges of risks and threats are vital to protecting critical infrastructures for the future and overall sustainability. This work reviews and summarizes current research and standards, the state of the art, and an empirical study with critical infrastructure experts that are responsible for risk management of their respective critical infrastructures. The research questions we asked summarized the following takeaways. For RQ1, we found that trustworthy assets and configuration knowledge are challenged by organizational challenges (e.g. fragmented data needs, legacy systems, inconsistent inventories) and technical limitations (e.g. risks of active scanning of OT environments). For RQ2, supplier risk management has limitations regarding fragmented regulations, lack of transparency in deep-tier supply changes, and the "dependency trap". For RQ3 key takeaway, effective operationalization of asset and supplier intelligence needs the integration of both technical and business-related data to align and in turn optimize automated systems that validate information and help create risk-based mitigation actions in key situations. Overall, there are limitations. Because this topic evolves rapidly, some practices or state-of-the-art methods, or standards can change and may not be included. Also, the qualitative approach includes a risk of a researcher bias despite attempts to maintain objectivity, accuracy, and reliability. Our findings are based on 11 interviews with four CI operators in central Europe and therefore provide in-depth practice insights rather than broad generalizability. Moreover, the demonstrator remains in development and has not yet been fully implemented or evaluated. Nevertheless, this paper summarizes the existing challenges and presents an overview and potential demonstrator solution, which authors intend to implement and evaluate in future work.

7 Acknowledgements

This work was funded by the German Federal Ministry of Education and Research (BMBF; now operating as the German Federal Ministry of Research, Technology and Space, BMFTR) within the framework of the call "Bedrohungen aus dem digitalen Raum" as part of the federal program "Forschung für die zivile Sicherheit". It was carried out in the project AeroKI – Ermittlung von Bedrohungslagen in Kritischer Infrastruktur am Beispiel von Flughäfen [Bu23].

Bibliography

[AL24] Ali Milaat, F.; Lubell, J.: Layered Security Guidance for Data Asset Management in Additive Manufacturing. Journal of computing and information science in engineering and 24(7)/2024, 071001, 2024.

[Al20] Alén, S.: Development of a CMDB Model to Represent SaaS Organization Assets Relevant for Service Delivery. 2020.

[BC23] Braun, V.; Clarke, V.: Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. Int. J. Transgender Health, Bd. 24, Nr. 1, pp. 1–6, 2023.

[Bo22] Boyens, J. et.al.: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. National Institute of Standards and Technology, NIST Special Publication (SP) 800-161 Rev. 1. 2022.

[BS24] Bowen, F.; Siegler, J.: The role of visibility in supply chain resiliency: Applying the Nexus supplier index to unveil hidden critical suppliers in deep supply networks. Decis. Support Syst., Bd. 176, 2024.

[Bu23] Bundesministerium für Bildung und Forschung (BMBF): Ermittlung von Bedrohungslagen in kritischer Infrastruktur am Beispiel von Flughäfen (AeroKI). In: SIFO.de - BMBF-Sicherheitsforschung, September 2023. Internet: https://www.sifo.de/sifo/shareddocs/Downloads/P-Umrisse/projektumriss_aeroki.pdf?__blob=publicationFile&v=2 , 06.05.2026.

[Bu25] Bundesgesetzblatt Teil I - Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. 2025.

[CCM18] Colicchia, C.; Creazza, A.; Menachof, D. A.: Managing cyber and information risks in supply chains: insights from an exploratory analysis. Supply Chain Manag. Int. J., Bd. 24, Nr. 2, pp. 215–240, 2018.

[CI26] CISA: Software Bill of Materials (SBOM) - CISA. https://www.cisa.gov/sbom, accessed: 11/02/2026.

[Cu22] Cui, L. et.al.: Improving supply chain collaboration through operational excellence approaches: an IoT perspective. Ind. Manag. Data Syst., Bd. 122, Nr. 3, pp. 565–591, 2022.

[Cy26] CyberSecTools: https://cybersectools.com/, accessed: 12/02/2026.

[DM03] Dulmin, R.; Mininno, V.: Supplier selection using a multi-criteria decision aid method. J. Purch. Supply Manag. and 9(4)/2003, pp. 177–187, 2003.

[Ed19] Edgar, T. W. et.al.: Safer and optimised vulnerability scanning for operational technology through integrated and automated passive monitoring and active scanning. Journal of Information Warfare and 18(4)/2019, pp. 125-155, 2019.

[El21] El-Garaihy, W. H.: Analysis of supply chain operations reference (SCOR) and balanced scorecard (BSC) in measuring supply chains efficiency using DEMATEL and DEA techniques. J. Glob. Oper. Strateg. Sourc., Bd. 14, Nr. 4, pp. 680–700, 2021.

[Fe21] Federal Office for Information Security: Second act on increasing the security of IT systems (German IT Security Act 2.0), 2021.

[Fr25] Friedman, R. P.: Factors Shaping Policy for Cybersecurity Resilience in Critical Infrastructure (CI) Organizations: Proposing an Adaptive Cyber Resilience Policy Model (ACRPM). Liberty University, 2025.

[GKS05] Gelle, E.; Koch, T. E.; Sager, P.: IT asset management of industrial automation systems. In (ed.): Proc. 12th IEEE Int. Conf. and Workshops on the Engineering of Computer-Based Systems (ECBS'05). pp. 123–128, 2005.

[Go15] Govindan, K. et.al.: Multi criteria decision making approaches for green supplier evaluation and selection: a literature review. J. Clean. Prod. and 98/2015, pp. 66–83, 2015.

[Go23] Govindan, K. et.al.: Analysis of supplier evaluation and selection strategies for sustainable collaboration: A combined approach of best–worst method and TOmada de Decisao Interativa Multicriterio. Bus. Strategy Environ. and 32(7)/2023, pp. 4426–4447, 2023.

[HXD10] Ho, W.; Xu, X.; Dey, P. K.: Multi-criteria decision making approaches for supplier evaluation and selection: A literature review. Eur. J. Oper. Res., Bd. 202, Nr. 1, pp. 16–24, 2010.

[JK25] Joswig, T.; Kurz, W.: Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany. Journal of Next-Generation Research 5.0, 2025.

[KD25] Kayouh, N.; Dkhissi, B.: Evaluating Supplier Supply Chain Performance Using a Multi-Criteria Decision-Making Approach: Case Study in the Automotive Industry. Manag. Prod. Eng. Rev. and 16(2)/2025, 2025.

[Ku03] Kujawski, E.: 4.7.3 Multi-Criteria Decision Analysis: Limitations, Pitfalls, and Practical Difficulties. INCOSE Int. Symp., Bd. 13, Nr. 1, pp. 1169–1176, 2003.

[MKG23] Modi, A.; Kuzminykh, I.; Ghita, B.: Data Driven Approaches to Cybersecurity Governance for Board Decision-Making - A Systematic Review. 2023.

[Mo23] Mohammed, I. A.: Artificial Intelligence In Supplier Selection And Performance Monitoring: A Framework For Supply Chain Managers. Educ. Adm. Theory Pract. and 29/2023, 2023.

[Ol25] Olech. A.: Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses. Terroryzm – studia, analizy, prewencja Special Issue/2025, 133-158, 2025.

[OOE25] Onukwulu, E. C.; Odochi-Agho, M.; Eyo-Udo, N. L.: Innovations in Supplier Evaluation: Frameworks and Techniques for Supply Chain Resilience. Int J Res Sci Innov IJRSI, Bd. 11, pp. 610–623, 2025.

[PDB24] Papamichael, M.; Dimopoulos, C.; Boustras, G.: Performing risk assessment for critical infrastructure protection. Sustain. Resilient Infrastruct., Bd. 9, Nr. 4, pp. 367–385, 2024.

[PKS23] Parkin, S.; Kuhn, K.; Shaikh, S. A.: Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception. Journal of Cybersecurity

and 9(1)/2023, tyad018, 2023.

[Sa22] Samanis, E. et.al.: SoK: A Taxonomy for Contrasting Industrial Control Systems Asset Discovery Tools. In (ed.): Proc. 17th Int. Conf. on Availability, Reliability and Security (ARES '22), New York, NY, USA. pp. 1–12, 2022.

[Se26] Secure-by-Design Handbook: IEC 62443 Series. www.securebydesignhandbook.com, accessed: 11/02/2026.

[Si23] Singh, P. K.: Digital transformation in supply chain management: Artificial Intelligence (AI) and Machine Learning (ML) as Catalysts for Value Creation. International Journal of Supply Chain Management and 12(6)/2023, pp. 57-63, 2023.

[St23] Stouffer, K. et.al.: Guide to Operational Technology (OT) security. National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-82r3, 2023.

[To21] Topping, C. et.al.: Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Comput. Secur., Bd. 108, 2021.

[Ve25] Venanzi, R. et.al.: Towards IT/OT integration in industry digitalization: A comprehensive survey. Journal of Network and Computer Applications and 104373/2025, 2025.

[WDG23] Wetzels, J.; Dos Santos, D.; Ghafari, M.: Insecure by design in the backbone of critical infrastructure. In (ed.): Proc. Cyber-Physical Systems and Internet of Things Week 2023. pp. 7-12, 2023.

[Wh16] White, R. et.al.: Towards a Comparable Cross-Sector Risk Analysis: RAMCAP Revisited. In (Rice, M.; Shenoi, S. eds.): Critical Infrastructure Protection X, Bd. 485. Cham: Springer, pp. 221–237, 2016.