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-p27850-cd

Engineering Cyber Resilience Under Resource Constraints for Critical Infrastructure Protection

Ebba Linnea Nilsson

Department of Computer Science, Electrical and Space Engineering (SRT) Division: Digital Services and Systems, Luleå University of Technology, Sweden.

Hampus Ettehag

Department of Computer Science, Electrical and Space Engineering (SRT) Division: Digital Services and Systems, Luleå University of Technology, Sweden.

Christine Große

Department of Computer Science, Electrical and Space Engineering (SRT) Division: Digital Services and Systems, Luleå University of Technology, Sweden, E-mail: christine.grosse@ltu.se.

This research is situated at the intersection of cybersecurity risk management and critical infrastructure protection, where traditional security approaches are challenged by evolving threats and resource constraints. Although consequence-driven cyber-informed engineering (CCE) offers a powerful methodology for protecting critical infrastructure, its resource requirements challenge organizations with limited financial capacity, personnel availability, or technical expertise, for example municipalities operating water supply and wastewater treatment. This paper addresses the fact that no simplified version of CCE exists that, while requiring fewer resources to implement, maintains the essential protective capabilities. This study investigates the principles of CCE and how adaptation to resource constraints can be feasible to strengthen smaller organization's ability to handle cyber threats and maintain public services. To this end, the CCE and the literature on cyber resilience, resource constraints and organizational adaptation strategies are examined about resource requirements, specific characteristics and suitable proposals for adaptations. The results also provide valuable insights into municipal wastewater practice. The paper contributes a comprehensive outline of the CCE and recommendations for practice on how to adapt this framework to be more attainable for organizations with limited resources. It highlights the potential of the adapted CCE to reduce resource requirements while maintaining the fundamental protection logic.

Keywords: Consequence-driven, resilience engineering, cyber resilience, critical infrastructure, public service, local governance, wastewater.

1. Introduction

As cyberattacks on infrastructure systems become increasingly sophisticated and frequent, organizations are under growing pressure to protect critical functions while operating within various resource constraints (Hossain et al. 2025). This has led to the recognition that preventing catastrophic consequences is more important than simply preventing cyberattacks (Bartusiak et al. 2024). As a result, the focus of security approaches is slowly shifting from preventing incidents to ensuring continuity, that is, mitigating unacceptable physical, economic, or societal impacts (Agbo & Mehrpouyan 2023).

One such method, consequence-driven cyber-informed engineering (CCE), focuses on avoiding the aforementioned consequences and integrates cybersecurity into engineering practice (Bochman & Freeman 2021). However, even such approaches that prioritize the protection of critical functions, are seen too complex or resource-intensive for public organizations that manage critical infrastructure (CI) and must balance the need for stringent security measures with limited resources. This paper addresses the need for multi-disciplinary efforts for an adapted security methodology (Tuptuk et al. 2021) and explores how the CCE method can be adapted to maintain its robust protective capabilities while considering and adapting to the resource constraints of municipal CI operators.

2. Background

2.1. *Critical infrastructure resilience*

Critical infrastructure is a complex socio-technical system-of-systems providing essential societal functions (Große 2023; Rinaldi et al. 2001). Modern societies are increasingly interconnected and dependent on such functions (Große 2023), including water supply and wastewater treatment. Its reliable operation depends not only on physical assets, but also on the management of the interrelationships among its technical and social components at multiple levels (Große 2023; Rinaldi et al. 2001).

The digitalization of control mechanisms has led to an increase in attack vectors, requiring strategies specifically tailored to the operational conditions and security requirements of CI (Johnson & Edwards 2007). Proactive adaptation to maintain critical functions under stressful conditions is often referred to as resilience engineering (Hollnagel et al. 2006). The inability of a system to adapt to the complexity and variability of the real world is seen as failure (Madni & Jackson 2009; Hollnagel et al. 2006). The focus is on how organizations can monitor risk profiles and find appropriate trade-offs between safety requirements and operational constraints, using four capabilities to describe resilient systems: anticipation, monitoring, response, and learning (Madni & Jackson 2009).

Furthermore, cyber resilience goes beyond traditional cybersecurity by ensuring that organizations can identify appropriate measures to mitigate the risks associated with CI disruptions (Bartusiak et al. 2024). It emphasizes that organizations must be able to maintain service operations during incidents and includes both preventive measures and the ability to operate in alternative ways when digital systems are compromised (Ohrt et al. 2021). Consequence-driven approaches like the CCE help to shift the focus on the continuity of CI operation (Bochman & Freeman 2021; Agbo & Mehrpouyan 2023).

2.2. Resource-based view

Resource constraints affect organizations' ability to implement effective security measures. The resource-based view provides a systematization into three categories (Barney 1991): physical resources that support operations, human resources, including the skills and competencies of staff, and organizational resources that enable coordination and management. Furthermore, resources and their use must be understood in the respective operational context (Barney 2001). In addition, financial constraints have cascading effects on all three categories, as they limit the ability to hire qualified personnel, maintain fixed assets, and implement necessary security controls. They can also lead to delays in important system upgrades and security enhancements (Tuptuk et al. 2021), resulting in a reactive security posture where resources are only increased after an incident has occurred.

Resource constraints are particularly relevant in the context of local public services. In Sweden, 83 out of 290 municipalities reported negative financial results in 2024 (SCB 2025), suggesting that they face challenges in implementing comprehensive cybersecurity measures associated with limited budgets.

2.3. *Wastewater treatment context in Sweden*

Swedish municipalities are often also responsible for the operation and maintenance of wastewater treatment systems and thus for their protection (Svenskt Vatten 2026). Apart from physical security, the wastewater sector lags significantly behind other sectors in the implementation of cybersecurity measures, as it has never been subject to the same security standards as other infrastructure and lacks resources. However, wastewater treatment is now considered CI for public health and the local economy. Technological advances have improved operational efficiency and availability, but at the same time increased vulnerability to cyberattacks (Johnson & Edwards 2007). In addition, many plants still operate with outdated system devices and firmware versions that were developed decades ago (You 2022). The switch to remote control increases the challenges (You 2022).

In sum, a comprehensive security concept for such organizations must balance robust cybersecurity with operational requirements.

3. Methodology

This study used a thorough and well-founded approach to analyze both the CCE methodology and the problems associated with its practical application, as well as suitable adjustments. By integrating document analysis and expert knowledge from a municipal wastewater plant, this single-case qualitative study encompassed a variety of theoretical and practical material, which increased credibility and reduced bias

(Bowen 2009). The triangulation of data helped to combine it to comprehensively examine the phenomenon (Bowen 2009) and ensure consistent conclusions (Leedy et al. 2021).

The document analysis covered CCE methodology documentation, sector-specific documentation, implementation guidelines in various contexts, and case studies from practical CCE implementations. Careful analysis of these documents provided a fundamental understanding of the CCE methodology, relevant industry standards, and areas for improvement based on previous implementations. It also formed the basis for the interview questions, including new insights that needed further investigation (Bowen 2009).

The study involved experts in eight semi-structured one-to-one interviews, seven feedback and discussion rounds in groups and eight validation workshops. To ensure reliability and relevance, participants were selected through purposive sampling (Patton 2015), using a set of criteria that prioritized sector-specific expertise, professional, policy, or regulatory experience, academic background, and practical involvement in CCE.

Based on document analysis, considering the CCE and its resource requirements, we created a breakdown artifact that details the input, objective, content and output of each phase of the CCE. By iterative thematic coding, the empirical study in the context of a municipal wastewater organization investigated the circumstances of the practical implementation of the CCE, feedback mechanisms and collaboration issues, and the resource requirements of each phase. Analysis of the empirical material consolidated six resource categories: financial, human, organizational, technological, physical, and time resources. The resource intensity for each phase and category was assigned by expert assessment on a scale of 1 to 5, which was then discussed during the validation workshops to reach consensus. This approach ensured that the analysis was theoretically sound, grounded in practical experience, reflected real-world challenges and provided relevant adaptations of the CCE to resource-constrained organizations.

4. A Resource-based View on CCE

4.1. *Breakdown of the CCE phases*

The CCE focuses on identifying and mitigating the most serious consequences of cyberattacks, rather than simply trying to prevent them. The core principle is to protect the functions most critical for fulfilling an organization's purpose, focusing on high consequence events (HCEs) (Bochman & Freeman 2021). Table 1 shows the breakdown for each CCE phase, using the results of the previous phase as input. It summarizes the objective of each phase, its main content as key activities (KA), and their results as output.

A fundamental assumption of CCE is that organizations targeted by advanced cyberattacks are likely to be compromised. Rather than focusing on preventing attacks, CCE seeks to minimize their impact through system design. Integrating security into system design includes both physical and digital controls that can reduce or eliminate cyber risks, rather than relying solely on retroactively applied IT security measures.

Another key component of CCE is system analysis to examine the dependencies and interconnections among different systems to understand the cascading effects of cyberattacks. The development of protection strategies is thus an important part of CCE. It encompasses both technical and organizational measures to significantly reduce the impact of HCEs and ensures that CI remains resilient even in the face of sophisticated cyber threats (Bochman & Freeman 2021). This also includes an appropriate organizational perspective on cybersecurity to enhance how employees understand and handle cyber risks.

The CCE consists of four main phases preceded by a preparatory phase, which is optional but can save resources during Phases 1 to 4. It includes activities such as training, scoping, data protection plans, a common taxonomy, teams and other agreements. It also includes defining roles, responsibilities, logistical details such as site visits and resource allocation (Bochman & Freeman 2021).

Consequence prioritization is the first phase of the process and aims to identify the most serious disruptions, particularly cyber-induced events, and to understand which failures of essential functions would be catastrophic for the organization's mission (Bochman & Freeman 2021). This assumes that an attacker already has access to the organization's systems and can cause disruptions. The team assesses the potential consequences, considering factors such as the number of people or systems affected, the costs of recovery, the risks to public safety, the ability to restore system integrity, and the duration of the disruption (Bochman & Freeman

2021). To ensure a consistent assessment, a weighted scoring system is used. Factors such as safety, financial impact, and system integrity are assigned numerical values, with the most damaging events receiving higher scores. Only the most serious events are classified as HCEs and proceed to the next phase of analysis.

Table 1. Detailed breakdown of the CCE phases.

Phase 1	**Consequence Prioritization**
Input	Scoping and Contracts Data Agreements and Connections Data Management and Architecture Plan Trained Assessment Teams
Objective	Identify HCEs that could disrupt the provision of critical public services.
Content	[KA1.1] Define objectives, scope and boundary conditions [KA1.2] Determine Severity Criteria [KA1.3] Identify potential adverse events [KA1.4] Score the severity of potential (cyber) events and identify HCEs [KA1.5] Achieve leadership concurrence
Output	List of validated and approved HCEs
Phase 2	**Systems Analysis**
Input	Output from Phase 1
Objective	Map and analyze the systems and processes related to the identified HCEs, gathering information exploitable for triggering those events.
Content	[KA2.1] Translate HCEs into Block Diagrams [KA2.2] Develop functional descriptions [KA2.3] Collect and organize data [KA2.4] Create a functional data repository [KA2.5] Produce a preliminary system description [KA2.6] Protect access and implement document control for the assessment
Output	A map and analysis of the systems and processes related to the identified HCEs, including block diagrams, functional descriptions, and a functional data repository for each HCE
Phase 3	**Consequence-based Targeting**
Input	Output from Phases 1 and 2
Objective	Identify areas where security is assumed without validation. Develop and validate high-confidence kill chains, mapping potential cyberattack sequences
Content	[KA3.1] Identify technical target [KA3.2] Describe technical approach [KA3.3] Develop kill chains/CONOPS [KA3.4] Identify and define critical information needs [KA3.5] Brief leadership
Output	Kill chains for each HCE
Phase 4	**Mitigations and Protections**
Input	Output from Phases 1 and 3
Objective	Identify and develop protection strategies to mitigate attack paths identified before.
Content	[KA4.1] Brainstorm potential measures [KA4.2] Map potential measures to the NIST functions [KA4.3] Validate potential strategies [KA4.4] Present security strategies to leadership [KA4.5] Develop adversary tripwires
Output	Document outlining recommended operational, procedural, and technical design changes

The systems analysis, Phase 2 in CCE, compiles critical information to understand how adversaries could exploit systems to trigger HCEs. The goal is to map the assets, tools, and processes by creating high-level diagrams to visualize the relationships between cyber manipulation and a HCE and developing a functional repository for further analysis. Understanding system access points, patching processes, software versions, and vendor dependencies is critical to building a comprehensive picture of vulnerabilities. In addition, understanding human factors and access policies for contractors and suppliers is essential to assessing potential security gaps (Bochman & Freeman 2021). However, the work and findings of this phase must be carefully organized and protected, as they also can provide adversaries with a valuable roadmap for an attack (Bochman & Freeman 2021).

Phase 3, consequence-based targeting, identifies areas of unverified trust, i.e. areas where trust is based on incomplete knowledge within a system to determine plausible attack paths and uncover vulnerabilities that even strong defenses may not be able to prevent (Bochman & Freeman 2021). The CCE Kill Chain, increases attack scenario realism by adopting a hostile mindset. In an iterative, team-based approach with key roles, analysts assess how attackers gather information, identify access points, and plan their actions, often using trusted external entities like vendors or subcontractors to obtain critical information (Bochman & Freeman 2021). Validated attack scenarios must realistically consider system

physics, technical feasibility, and access paths, including network, human, and supply-chain entry points. A detailed adversarial collection plan is created that outlines how an attacker would gather the information necessary to execute the attack. The effectiveness of the next phase depends on the accuracy and completeness of this phase.

Phase 4 regards mitigation and protection against the defined attack scenarios. The CCE team conducts workshops to explore mitigation approaches, resulting in a documented set of operational, procedural, and technical design changes. The core principle here is to eliminate digital vulnerabilities through engineering solutions, emphasizing non-digital control mechanisms for all digitally controlled processes that could have unacceptable physical consequences. Monitoring is only implemented if digital dependencies cannot be eliminated or if it provides essential awareness at critical bottlenecks. This approach is consistent with the NIST cybersecurity framework; however, CCE gives priority to protection through non-digital remedies, such as human oversight in decision-making (Bochman & Freeman 2021). Industrial control systems also feature traditional safety devices that provide inherent protection against cyber threats. Examples include pressure relief devices, mechanical overspeed trips, check valves, motor monitoring devices, and analog instrument loop monitors (Bochman & Freeman 2021). While these safeguards can cause operational disruption, they prevent catastrophic damage or destruction. In addition to specialized industrial protection systems, these measures protect expensive, hard-to-replace equipment, especially from attacks targeting multiple similar systems (Bochman & Freeman 2021).

4.2. *Insight into CCE in a municipal context*

Based on testing CCE in a municipal wastewater treatment organization, this study analyzed challenges and possibilities for each phase, focusing in particular on resource consumption and opportunities for adapting the CCE method, including feedback mechanisms and collaboration issues that may impact CCE implementation in organizations with limited resources.

Participants noted that while the first phase requires effort, it is generally less resource-intensive than the Phases 2 and 3. However, there are challenges in securing initial buy-in and ensuring that CCE teams are sufficiently informed about the methodology and the need for an adversarial mindset, which is considered difficult for personnel. In Phase 1, feedback mechanisms include regular meetings to build understanding of the methodology used and the cybersecurity strategy of the organization, as well as workshops and iteration sessions. If the initial scoring (KA1.4) does not seem accurate, follow-up discussions allow for reassessment. Issues that may arise include the identification of inefficiencies, outdated documentation, and system mapping gaps, which may require added effort. In addition, there may be friction between teams, but also improved collaboration and communication, leading to a unified cybersecurity approach and smarter resource allocation. This phase involves extensive data collection and stakeholder interviews across departments, requiring careful coordination to reach consensus. Given the possibility of significant adjustments (e.g., severity scales) during this phase, an iterative approach is considered important to achieve a workable outcome. A perceived pressure to rapidly arrive at a conclusion can sometimes compromise analysis and lead to misplaced priorities or an unclear scope. Unexpected insights gained during this phase can also help to refine priorities and make more informed decisions about resources. The sensitivity of the information discussed also requires adequate attention.

Phase 2 was rated as highly resource-intensive in all categories. In large organizations in particular, mapping system interdependencies and gathering information from different departments is likely to be a major challenge, which is heavily influenced by the maturity of the organization and the available system support. Organizational coordination often proves to be the biggest hurdle. Even though participants are already familiar with CCE at this stage, the process remains a substantial undertaking that requires a significant investment in staff time. Feedback loops in Phase 2 are incorporated in expert consultations, reviews of preliminary results, and the possibility of iterative refinement of data collection and analysis based on new findings. The municipal wastewater treatment experts suggested leveraging the knowledge of operational staff. They also advocated an iterative approach, initially analyzing systems at a superficial level and then gradually increasing granularity according to resource availability. Potential coordination issues include increased

interdepartmental cooperation and unexpected findings from the analysis of system interdependencies. Conversely, friction between teams due to differing priorities or perspectives can also arise, affecting resource use and process effectiveness. Moreover, the high sensitivity of the system data gathered during this phase necessitates robust information security practices.

Phase 3 is iterative by nature, with refinements and additions to be expected. Feedback mechanisms include meetings to determine details and discussions with management about progress and attack scenarios. This phase has been described as almost as resource intensive as Phase 2, as it often requires numerous workshops to establish a common view of potential attack vectors. One of the biggest challenges was guiding participants to consciously think like an attacker, which respondents found counterintuitive. They reported that successfully completing this phase requires a combination of different expertise: in-depth system knowledge coupled with an understanding of how systems can be disrupted. Compared to Phase 2, less cross-organizational coordination may be needed, provided that the relevant staff are already involved. Such adaptation to the perspective of potential attackers and cross-team collaboration can lead to both conflict and enhanced cooperation among analysts. However, unexpected findings can reveal hidden system dependencies, vulnerabilities, and attack vectors, thereby improving understanding of cyber risks including awareness of threats and consequences.

The participating experts generally agreed that Phase 4 required the least resources. One of the reasons given for this was that participants automatically think about solutions in the earlier, problem-oriented phases, thereby developing initial ideas for risk mitigation. The main task here is to systematically evaluate the numerous proposals and identify the most effective measures, with preference given to non-digital or engineering-based controls ("cyber-free solutions"). The alignment of solutions with frameworks such as NIST was also cited as an important means of strengthening structure and completeness. Feedback mechanisms are thus linked to review meetings, expert consultations, and penetration tests to validate the effectiveness of remedial measures. The potential for learning can arise from collaboration between security and engineering teams, leading to increased awareness of cyber risks, proactive identification of vulnerabilities, and a broad range of remediation measures in an organizational context.

4.3. *Resource intensity of CCE*

The assessment of resource intensity for each CCE phase was based on six categories: financial, human, organizational, technological, physical, and time resources (see Table 2).

Table 2. Resource-based view on the CCE phases.

Category	Justification – Phase 1	Level
Financial	Extensive data collection, incl. interviews, thinking, opinions	4
Human	Availability of people. Possible lack of training in CCE. Difficult to create engagement.	5
Organizational	Establishing a common ground for the organization, not only group by group.	3
Technological	Low technical demand.	1
Physical	Low physical needs.	1
Time	Time allocation and due dates.	5
Category	**Justification – Phase 2**	**Level**
Financial	It reflects the other categories.	5
Human	Various professionals are required. The process usually runs smoothly, even though the task is complex.	4
Organizational	Compiling information across the organization is demanding. Dependent on maturity level.	5
Technological	Manage all information	5
Physical	Facilitate many meetings and workshops	4
Time	Time consuming for participants	5
Category	**Justification – Phase 3**	**Level**
Financial	Similar to Phase 2	5
Human	Challenging to maintain an attacker perspective and prioritizing scenarios.	4
Organizational	Cross-departmental teams are established since before.	4
Technological	Similar to Phase 2	5
Physical	Similar to Phase 2	4
Time	Discussion of detailed scenarios	5
Category	**Justification – Phase 4**	**Level**
Financial	It reflects the other categories.	3
Human	Availability of professionals to handle the scenarios	3
Organizational	Alignment with policies and third-party agreements	2

Technological	Systematic assessments of possible solutions	3
Physical	Less need for gatherings.	1
Time	Consolidation work is required.	2

Phase 1 showed high intensity in terms of human and time resources, primarily due to the number of interviews to be conducted and the need to involve stakeholders. The analysis revealed that Phases 2 and 3 were the most resource-intensive overall. Phase 2 received the highest rating for all resource requirements. One reason cited for this was the challenge of gathering information from across the organization. Phase 3 was also very demanding in terms of human, organizational, technological, and time resources, similar to Phase 2, particularly for workshops that were necessary to achieve a common understanding about scenarios and find common ground. In contrast, Phase 4 was generally rated as less resource-intensive, particularly in financial and physical terms, as much of the analytical work had been completed in earlier phases and known security measures had been applied. This suggests that the main resource expenditure in CCE lies in the detailed preparation, analysis, and data collection phases, as summarized in Table 2. It should also be recognized that these activities, which are perceived as resource-intensive, not only contribute to the results in the CCE, but also pay off in incident response cases, as they substantially improve the decision-making abilities of the individuals involved. Attempts to reduce resources in these phases must therefore account for the associated secondary risks.

5. Discussion

5.1. *Adaptions of CCE to municipal conditions*

The results from the analysis, testing and refinement of the CCE in a municipal wastewater treatment context, allowed several adjustments to the CCE to be proposed for such conditions. The most promising adaptations, as determined by the participants' high scores, are presented here.

Regarding Phase 1, the use of a structured brainstorming template to identify HCEs was preferred because it offers high potential for increasing effectiveness, especially in helping participants adopt an adversarial mindset, although it was recognized that this could still be challenging for non-security professionals.

For Phase 2, multiple adjustments aimed at streamlining the system analysis by initially focusing on critical systems and utilizing existing data resonated well. These were appreciated for their effectiveness and resource efficiency, with suggestions that an iterative approach would be beneficial to balance focus with completeness.

In Phase 3, prioritizing the most critical technical targets received the most support, indicating strong agreement on their feasibility, effectiveness, and resource efficiency. The use of existing knowledge bases (e.g. MITRE ATT&CK) to describe the technical approach was also highlighted. Starting with non-cyber scenarios was also recognized as valuable in this phase.

For Phase 4, focusing brainstorming on cost-effective remediation measures was considered most important, with experts noting that examples could aid in idea generation. Adjustments for mapping to NIST and validating countermeasures also received strong support. Feedback suggested that these could potentially be combined with the former to further increase efficiency. Prioritizing the development of tripwires for critical areas was also considered a worthwhile adjustment.

The proposed and expert-evaluated adaptations of the CCE are consistent with the existing literature on adapting complex frameworks to resource-constrained environments. The adapted method incorporates several strategies such as focusing on essential activities, prioritizing critical functions, leveraging existing organizational knowledge and existing tools, and emphasizing practical technical controls over potentially costly or complex digital solutions. The experts' positive assessments of feasibility and resource efficiency of the adaptations also underscore the relevance of these strategies in the CCE context.

Furthermore, the findings confirm the emphasis in the literature on the impact of resource constraints—particularly in terms of staff time, expertise, and financial capacity—on the implementation of cybersecurity in sectors such as wastewater treatment (Hossain et al. 2025; Tuptuk et al. 2021; Johnson & Edwards 2007). The adapted method directly attempts to mitigate these specific burdens identified in both the literature and the test and analysis conducted in this study.

5.2. *Implications for future research on CCE*

This study in the context of CI protection has demonstrated clear sector-specific benefits. However, it also had its limitations in terms of scope and coverage. For example, the expert-evaluated adaptations of CCE were not yet

implemented in operational practice as it would require another CCE process. Follow-up research could apply the adapted CCE in a similar or additional infrastructure area, collecting implementation metrics, usability data, and outcome-oriented assessments and comparing them with other frameworks in use. The role of adequate preparation, playbooks, and checklists in recurring assessments would be of special interest, as would the potential for reusing HCEs in scenario-based training for all employees.

In addition, further research could broaden the spectrum of expert participation to include organizations operating under different regulatory, technical or environmental conditions. This would help to assess the generalizability and adaptability of the proposed adaptations to CCE. Although the adapted phases have been evaluated as effective, it comes with a risk of oversimplification, especially if important threat vectors or (inter-) dependencies are overlooked in a limited analysis. Future studies should evaluate trade-offs and identify thresholds at which simplification is likely to lead to a deterioration in security outcomes. Moreover, using a threat-agnostic and cascading perspective can further align the adapted CCE with an all-hazards resilience approach, reinforcing the argument that it is unrealistic to try to prevent all physical and digital attacks. The inclusion of a criterion for cascade effects in Phase 1 could highlight this perspective when assessing the severity of HCEs.

6. Conclusion

The paper contributes a comprehensive analysis of CCE and recommendations for adaptations for organizations with limited resources, based on findings from municipal wastewater operations. Adaptions include streamlining activities, using templates and existing resources, prioritizing critical elements, and incorporating flexibility. The adapted CCE is particularly designed to be feasible despite limited resources through the following measures: limiting the scope to a few HCEs and critical systems, iterating the depth according to available resources, reusing existing documentation and routines, and leveraging the reuse potential of CCE results. Adapted CCE offers resource-constrained CI organizations an achievable and pragmatic way to improve their cyber and all-hazard resilience against HCEs and thereby to ensure their supply of critical services to other critical infrastructures and society.

References

Agbo, C.; Mehrpouyan, H. (2023). Achieving Cyber-Informed Engineering Through Bayesian Belief Network and Sensitivity Analysis. IEEE DSA, 260-271.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1), 99-120.

Bartusiak, A.: Seidl, F.; Lässig, J.; Nicolai, S.; Bretschneider, P. (2024). Enhancing Cyber Resilience in Energy Systems through Automated Attack Scenario Generation: A Toolchain Approach. *IEEE SEST*, 1-6.

Bochman, A.A.; Freeman, S. (2021). *Countering cyber sabotage: introducing consequence-driven, cyber-informed engineering (CCE)*. CRC Press.

Bowen, G.A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27-40.

Große, C. (2023). A Review of the Foundations of Systems, Infrastructure and Governance. Safety Science, 160, 106060.

Hollnagel, E.; Woods, D.D.; Leveson, N. (2006). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

Hossain, S.T.; Yigitcanlar, T.; Nguyen, K.; Xu,Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges, *Urban Governance*, 5(1), 1-19.

Johnson, S.; Edwards, D. (2007). Why water and wastewater utilities should be concerned about cyber security. *J Am Water Works Ass*, 99(9), 89-94.

Leedy, P.D.; Ormrod, J.E.; Johnson, L.R. (2021). *Practical research: Planning and design*. Pearson.

Madni, A.M.; Jackson, S. (2009). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal*, 3(2), 181-191.

Ohrt, A.; Groves, D.A.; Cox, J.; Bochman, A.; Cunningham, C.; Hildick-Smith, A.; Kuczynski, T.L. (2021). Engineering Cyber–Physical Resilience. *J Am Water Works Ass*, 113(4), 32-40.

Patton, M. Q. (2015). *Qualitative research & evaluation methods*. SAGE Publications.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11-25.

SCB (2025). Annual accounts for municipalities and regions. Statistics Sweden.

Svenskt Vatten (2026). Verksamhetsstyrning. https://www.svensktvatten.se/vara-sakomraden/organisation-och-styrning/verksamhetsstyrning/.

Tuptuk, N; Hazell, P.; Watson, J; Hailes, S. (2021). A Systematic Review of the State of Cyber-Security in Water Systems. *Water*, 13(1), 81.

You, J. (2022). Strengthening cybersecurity of water infrastructure through legislative actions. *J Am. Water Resources Ass*., 58(2), 282-288.