Digital Twins for Essential Services

Alessio Bucaioni[a], Jakob Axelsson[a], Moris Behnam[a], Enxhi Ferko[a]

[a] *Mälardalen University, Västerås, Sweden*

Abstract

Digital twins, dynamic digital representations of physical systems, are emerging as transformative tools for enhancing crisis preparedness and resilience in critical societal sectors. By enabling real-time monitoring, simulation, and optimization, these technologies offer actionable insights to support proactive risk mitigation, efficient resource allocation, and continuous improvement of crisis response strategies. This study provides a comprehensive knowledge overview of digital twins, focusing on their applicability and impact in key sectors such as energy, healthcare, and transportation. Specifically, it examines the essential services most suited for digital twin adoption, the role of safety-critical data throughout their life-cycle, and their utility in identifying and mitigating risks within critical infrastructure. We employed a mixed-methods research design, combining systematic and gray literature reviews with expert interviews to integrate academic insights with practical perspectives. The findings reveal significant opportunities for digital twins to enhance operational efficiency, strategic planning, and crisis management. However, practical implementation remains in its infancy, with challenges related to cost, complexity, and limited real-world applications. In addition, this study provides actionable recommendations for stakeholders, emphasizing investment in digital twin technologies, robust data governance, and the development of standardized protocols. Future research directions include exploring applications of DTs in emerging sectors, such as crisis preparedness and societal resilience, advancing artificial intelligence integration, and adopting a system-of-systems perspective to address societal challenges comprehensively.

Keywords: Digital Twins, essential services, crisis preparedness.

1. Introduction

Digital Twins (DTs) are dynamic, digital representations of physical entities or systems that enable real-time monitoring, simulation, and optimization [?]. By bridging the physical and digital worlds, DTs allow for enhanced understanding, prediction, and decision-making, which have proved to be useful in many industries. It also makes them highly relevant for essential societal services where resilience and adaptability are crucial [P1, P6].

The integration of DTs into the management of essential services offers a range of possibilities, from modeling complex infrastructures to simulating disaster scenarios and testing response strategies. These capabilities are particularly vital for essential services such as energy, healthcare, and transportation [P3, P4]. By leveraging real-time data and advanced analytics, DTs can provide stakeholders with actionable insights, enabling more proactive risk mitigation, efficient resource allocation, and continuous improvement of response mechanisms for essential services.

Recognizing these opportunities, the Swedish Civil Contingencies Agency[1] (MSB) has outlined a strategic research agenda for 2024–2028, focusing on ten essential knowledge areas to address societal challenges and enhance the resilience of essential services. In autumn 2023, MSB initiated several actions to implement this agenda, including a call for knowledge overviews to consolidate insights and identify research gaps requiring further investment. Among the thematic priorities identified by MSB, the exploration of Digital Twins (DTs) has emerged as a significant area of inquiry due to their transformative potential in supporting essential services.

This study was conducted to provide such a comprehensive knowledge overview of DTs, focusing on their applicability and impact in the context of essential services. Through this examination, it aims to establish a foundation for understanding the role of DTs in enhancing the robustness of essential systems and identifying avenues for future research and practical application.

This study is guided by three key Research Questions (RQs):

- *RQ1: Which essential services are most amenable to DT development?* This question seeks to identify areas such as energy, healthcare, and transportation where DTs can provide the most significant benefits. The objective is

Email addresses: alessio.bucaioni@mdu.se (Alessio Bucaioni), jakob.axelsson@mdu.se (Jakob Axelsson), moris.behnam@mdu.se (Moris Behnam), enxhi.ferko@mdu.se (Enxhi Ferko)

[1] https://www.msb.se/en

to assess how DTs can strengthen civil protection and enhance the resilience of essential services.

- *RQ2: What role does safety-critical data play in the development and ongoing maintenance of DTs?* Here, the focus is on evaluating the importance of safety-critical data for the lifecycle of DTs, encompassing their development, deployment, and maintenance. Particular attention is given to data acquisition, management, and governance, with an emphasis on ensuring data security, integrity, and accessibility to maintain reliable and trustworthy digital representations.
- *RQ3: How can DTs be utilized in identifying, evaluating, and mitigating risks within essential services?* This question explores the use of DTs as tools for risk management, including the identification, evaluation, and mitigation of vulnerabilities in essential services. It examines how DTs can simulate scenarios, test strategies, and refine management protocols to enable proactive planning and efficient resource allocation.

To address these RQs, we employed a mixed-methods research process comprising a systematic literature review (SLR), a gray literature review, and expert interviews. The SLR was conducted to establish the current state of the art by analyzing peer-reviewed scientific publications. Acknowledging the importance of gray literature (such as blogs, white papers, and other practitioner-focused sources) in capturing the state of practice, we incorporated a gray literature review to bridge the divide between academic research and practical insights. Furthermore, we conducted expert interviews with stakeholders from industry and government to provide pragmatic insights, ensuring the development of actionable recommendations for enhancing essential services.

The main findings of our study are that DTs hold significant potential for enhancing the resilience, operational efficiency, and strategic planning of essential services. However, practical implementation remains limited, with current insights largely speculative or based on emerging applications rather than established practices. We identified actionable recommendations for stakeholders, emphasizing investment in DT technologies, data security, and standardized protocols, alongside the importance of evaluating long-term costs and benefits. Furthermore, our study highlights key directions for future research, including exploring DT applications in emerging sectors, such as crisis preparedness and societal resilience, integrating advanced AI techniques, and adopting a system of systems perspective to address societal challenges holistically.

The remainder of this study is organized as follows. Section 2 outlines the research process employed in the study. Sections 3, Section 4 and Section 5 provide detailed answers to the research questions. Section 6 discusses the main findings of the study. Section 7 provides an overview of the related work. Section 8 concludes with a summary of key findings, actionable recommendations for the private sector and industry, implications for government agencies, and directions for future research.

2. Research process

This study was designed and conducted following established guidelines for secondary studies in software engineering, as outlined by Kitchenham and Brereton [?]. To address the limitations of relying on a single method and enhance the validity of our findings, we incorporated a review of the gray literature, guided by Garousi's methodology [?], and conducted expert interviews based on Molleri et al.'s survey guidelines for software engineering research [?]. Our research process comprised three main phases: planning, conducting, and documenting, as illustrated in Figure 1.

Planning. The planning phase aimed to (i) establish the need for this study, (ii) define an overarching Research Goal (RG) and corresponding RQs, and (iii) develop a comprehensive research protocol to guide the systematic execution of the study. The output of this phase is a detailed research protocol outlining the key activities for the SLR, the gray review, and the expert interviews. Notably, the protocol specifies distinct sets of activities for each method: the systematic literature and gray reviews encompass activities labeled 5, 6, 7, and 8, while the expert interviews involve activities marked 13, 14, and 15.

Conducting. In the conducting phase, we implemented all activities outlined in the research protocol (activities 5 to 15). The process began with the search and selection step, where we conducted an automatic search of both peer-reviewed and gray literature. Selection criteria were defined and applied to filter the identified studies, resulting in a curated set of primary studies for further analysis. To ensure comprehensive coverage, the initial search was supplemented with exhaustive backward and forward snowballing, as recommended by Wohlin et al. [?]. Using the research questions as a foundation and systematically applying the standard key-wording process [?], we developed a set of parameters for classifying and comparing the primary studies. In the data extraction step, we analyzed each selected study to populate data extraction forms, which were subsequently aggregated for synthesis and analysis. During the data analysis step, both quantitative and qualitative methods were employed to examine the extracted data. The primary aim of this analysis was to comprehensively address the research questions and derive actionable insights. For the interviews, we followed Hackett et al.'s observation that interviews and questionnaires are among the most effective methods for collecting in-depth survey data [?]. The interviews were designed with open-ended questions to encourage detailed and nuanced responses. Invitations were sent to stakeholders from both industry and government, resulting in three expert interviews.

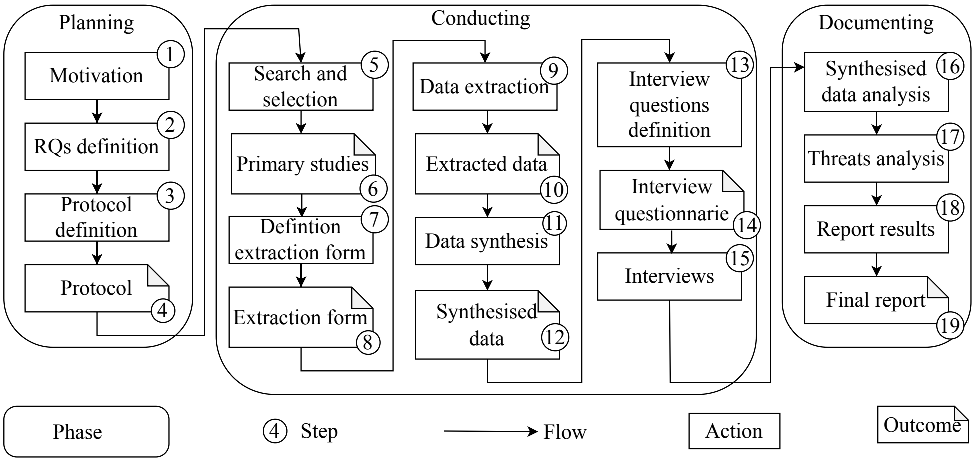

Figure 1: Overview of the adopted research method.

Documenting. In the documenting phase, we identified and documented potential threats to the validity of the study and recorded the results. To facilitate independent replication and verification of this work, we have provided a comprehensive and publicly available replication package[2]. This package includes the search and selection data, the complete list of primary studies, and the data extraction forms.

2.1. Search and selection strategy

By systematically following the steps outlined in Figure 2, we identified a total of 33 relevant primary studies for our investigation. Our approach involved two parallel

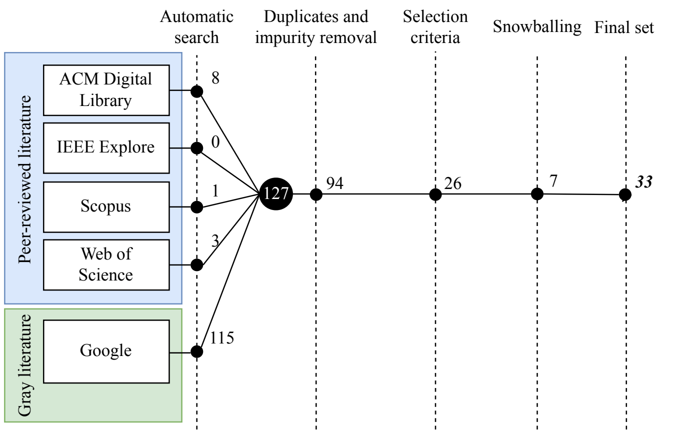

Figure 2: Overview of the search and selection process with number of potential studies for each step

reviews: one focusing on peer-reviewed literature and the other on gray literature. Both reviews adhered to a consistent process. For simplicity, we collectively refer to included studies from both sources as primary studies, unless otherwise specified. For the peer-reviewed literature, we selected four of the largest and most reputable scientific databases and indexing systems in software engineering: IEEE Xplore Digital Library, ACM Digital Library, Scopus, and Web of Science (Table 1). These databases were chosen for their high accessibility and strong track record in supporting systematic reviews in software engineering [**?** **?**]. It should be noted that during the automatic search for peer-reviewed literature, we excluded non-research papers, such as prefaces, editorials, or workshop summaries, by applying automated filters. This was feasible due to the small size of the academic corpus or the availability of reliable filtering mechanisms offered by some databases and indexing systems. For the gray literature search, we utilized Google, which accounts for 92.2% of global web searches, to ensure comprehensive coverage of practitioner-oriented sources (Table 1).

Table 1: Electronic databases, indexing systems and search engine used in this study

Name	**Type**	**URL**
IEEE Xplore Digital Library	Electronic database	http://ieeexplore.ieee.org
ACM Digital Library	Electronic database	http://dl.acm.org
Scopus	Indexing system	http://www.scopus.com
Web of Science	Indexing system	https://www.webofscience.com/wos/woscc/basic-search
Google	Search engine	http://google.com

We constructed the search string based on our overarching research goal and questions. The string was designed to be simple yet inclusive to maximize the retrieval of relevant studies. Threats to validity associated with the search string are discussed in Section 2.5. The search string used is:

[2]Replication package: https://drive.google.com/drive/folders/1b88EyuB_HloJc-oW5FOwISDwAfd2TYh7?usp=sharing

("Digital Twin" AND "Essential Services")

The search was conducted between January and March 2024, yielding an initial set of 127 potential primary studies. We adhered to the selection process proposed by Ali and Petersen [?], systematically removing impurities and duplicates before applying a predefined set of selection criteria. These criteria were designed to ensure an objective and rigorous filtering of the search results, as detailed below.

- Inclusion criteria
  1. Studies subject to peer-review (only for the peer-reviewed literature)
  2. Studies written in English
  3. Studies available as full-text
  4. Studies focusing on DTs
  5. Studies focusing on essential services
- Exclusion criteria
  1. Papers just mentioning DTs or essential services
  2. Peer reviewed studies (only for the gray literature)

It is worth noting that, although secondary studies are typically excluded in systematic reviews, we deliberately chose not to apply this exclusion criterion due to the limited size of the available peer-reviewed corpus in this emerging research area. We included in the next step only those studies that met all the inclusion criteria and none of the exclusion criteria. The selection criteria were iteratively applied to the title, abstract, and full text, resulting in a set of 26 potentially relevant studies. To minimize potential bias related to construct validity [?], we conducted a closed recursive backward and forward snowballing process [?].

This activity led to the identification of 7 additional peer-reviewed studies, resulting in a final set of 33 primary studies, 11 peer-reviewed and 22 gray literature sources. The complete list is provided in the appendix titled "Primary Studies."

It should be noted that, throughout the remainder of this work, we label peer-reviewed sources as P[·] and gray literature sources as G[·] for clarity and traceability.

2.2. Definition of the data extraction form

We designed the data extraction form, shown in Table 2, to systematically extract and collect data from the primary studies. The form consists of six clusters, each addressing specific aspects of the research questions identified in Section 1. For each category, we documented the relevant information from the primary studies as free-text entries. Notably, the extraction form was also validated by MSB, which deemed it sufficiently detailed to provide answers to the knowledge overview. To develop the extraction form, we employed a systematic keywording process [?]. Keywords and concepts were initially collected by thoroughly reviewing the full text of the primary studies. These keywords and concepts were then grouped into categories using a process inspired by the sorting phase of grounded theory methodology, involving open and axial coding [?]. The extraction form was iteratively refined to ensure completeness and accuracy. Revisions were made when new, relevant information was identified that was not already captured, or when certain categories were deemed non-viable due to a lack of data. After finalizing the form, we re-analyzed the primary studies using the refined structure and extracted additional data as necessary.

2.3. Interviews with experts

In this step, we followed the guidelines by Shull et al. [?] and conducted a total of three interviews. Interviews are widely recognized as one of the most effective methods for collecting comprehensive and nuanced data, particularly from practitioners across organizations [?]. We conducted semi-structured, in-depth interviews to gather qualitative data. This approach enhanced the depth of our findings [?] while mitigating threats to conclusion validity. The main aim of the interviews was to complement and extend our earlier findings with practitioner-oriented insights, particularly in identifying the areas perceived as most relevant for future investigation. Experts were selected based on their professional reputation and experience with digital twins and essential services. The expert pool comprised:

- I1: an expert in next-generation architecture within telecommunications systems, representing a multinational networking and telecommunications company.
- I2: a senior advisor leading the AI initiative for a multinational conglomerate based in Sweden.
- I3: an associate professor specializing in the maintenance and management of critical infrastructure at a technological university ranked among the top 20 in Europe and the top 100 globally.

Before the interviews, each participant received a preparation sheet detailing the interview's focus, estimated duration, and the privacy and confidentiality measures in place. The preparation sheet also included a summary of our preliminary findings, which served as a basis for discussion. The interviews were conducted remotely using Microsoft Teams[3]. For privacy reasons, we did not record the interviews; instead, the research team took anonymised notes during each session. During the sessions, participants were encouraged to freely focus on the topics they considered most significant. The interviews lasted between 30 and 45 minutes.

2.4. Data extraction, synthesis and analysis

We extracted, analyzed, and synthesized the data following the guidelines proposed by Cruzes et al. [?]. Our

[3]https://www.microsoft.com/en-us/microsoft-teams/group-chat-software

Table 2: Data extraction form

Cluster	Category	Relation to RQ	Final axial coding
Understanding DTs	DT definition	Cross RQs	–
	Difference with related concepts	Cross RQs	–
Essential services	Sector	RQ1	Utility management, Infrastructure and transportation services, Sector-wide essential services, Urban and environmental systems, Community and societal services
	Evaluation methodology	RQ1	Risk evaluation and management, Data-driven decision making, Urban and infrastructure planning, Optimization and monitoring
	Societal impact	RQ1	Resilience and security, Quality of life and sustainability, Equitable and informed access
	Interdependence	RQ1	Critical infrastructure interactions, Integrated planning and management, Technological enhancements for resilience
	Case study	RQ1	Security and risk management, Infrastructure and urban development, Energy management and sustainability, Digital twin implementation for planning and monitoring, Industrial optimization, Large-scale energy infrastructure management
	Contribution to resilience	RQ1	Advanced technological resilience, Infrastructure and operational resilience, Societal resilience and community support
Safety-critical data	Safety-critical data requirement	RQ2	Real-time monitoring and management, Threat detection and impact analysis, Data security and privacy
	Safety-critical assessment strategy	RQ2	Advanced threat simulation and resilience assessment, Threat dynamics and propagation analysis, Anomaly detection with Machine Learning (ML)
	Data security measure	RQ2	Threat detection and awareness, Adaptive security measures, Technological implementations for security, Comprehensive cybersecurity strategies
Risk identification and mitigation	Risk identification technique	RQ3	Advanced risk analysis and simulation, Surveillance and behavior analytics, Cybersecurity and threat mitigation, Predictive maintenance and operational resilience
	Risk mitigation strategy	RQ3	Advanced technological integration in risk management, Predictive maintenance and system optimization, Comprehensive disaster preparedness and response planning
System of systems (SoS)	Relevance of DTs in SoS	RQ3	System configuration and operational adaptability, trategic disruption management and resilience planning, Comprehensive integration and monitoring systems, Advanced data management and sectoral applications
	Application of DTs in SoS	RQ3	Advanced risk management and cascading impact analysis, Enhanced operational integration and system interoperability
Artificial Intelligence (AI) / ML	AI/ML integration technique	RQ3	Advanced defensive AI strategies, AI-driven security measures, AI and ML operational analytics, DT technology advancements

research incorporated both quantitative and qualitative analyses, combining content analysis [?] and narrative synthesis [?]. This mixed-methods approach enabled us to categorize and code our findings systematically. Content analysis provided structured classification, while narrative synthesis offered detailed explanations and interpretations, enriching our understanding of the results. To identify trends and gather insights for each cluster in the data extraction form, we employed a line-of-argument synthesis process [?]. Initially, we analyzed each primary study and interview individually to classify their main features. Subsequently, we examined the entire dataset collectively to uncover patterns and relationships. The extracted data were then grouped, cross-tabulated, and systematically compared across different facets of the data extraction form. To identify relationships between these facets, we utilized contingency tables, enabling us to extract and evaluate pairwise relations effectively. This multi-faceted approach ensured a comprehensive synthesis and interpretation of our findings.

2.5. *Threats to validity*

This study on the use of DTs in essential services was conducted following well-established guidelines for systematic research, including the creation of a rigorously validated research protocol. Despite these measures, we acknowledge potential validity threats that may have influenced the study. Below, we outline these threats and the mitigation strategies employed.

A key challenge in systematic reviews is ensuring that the selected studies are representative of the broader state of the art and practice. To address this, we conducted an extensive search across four major scientific databases and complemented this with a gray literature review to capture insights from the state of practice. Additionally, we employed closed recursive backward and forward snowballing to ensure comprehensive literature coverage. Language bias presents another potential threat, as only English-language studies were included. However, given that English is the *de facto* language for scientific publications in computer science and software engineering, this threat is considered minimal. The diversity of terminology used to describe DTs or essential services may have introduced some gaps in coverage, but this risk was mitigated through the gray literature review and expert interviews.

Internal validity was safeguarded by adhering to systematic guidelines across all research activities, including literature reviews and expert interviews. To ensure the accuracy of the extracted and synthesised data, we employed descriptive statistics and cross-analyzed various categories from the extraction form. Sanity checks were performed to identify and resolve inconsistencies, ensuring robust data handling throughout the study. However, the small sample size of experts interviewed poses a limitation. While the experts were carefully selected for their domain expertise and professional backgrounds, the limited number may restrict the generalizability of insights derived from the interviews. To mitigate this threat, we complemented interview findings with data from a broad literature base to ensure a balanced perspective.

Construct validity could be affected by the formulation of search strings for both peer-reviewed and gray literature searches. We addressed this by using a simple yet inclusive search string to maximize coverage while maintaining focus. All studies retrieved during the search process were rigorously screened against well-defined selection criteria to ensure the inclusion of relevant and high-quality sources.

To mitigate threats to conclusion validity, we systematically applied and documented clearly defined processes for each stage of the study. All authors collaborated in defining the extraction form, data extraction, and synthesis to maintain consistency and accuracy. Furthermore, we provided a complete and publicly available replication package to enable independent verification and replication of all study steps. This package and the iterative refinement of the extraction form based on primary studies ensured a comprehensive and reliable analysis.

3. Essential services amenable to DT development (RQ1)

In this section, we focus on identifying areas where DTs can provide significant benefits, addressing RQ1. This is achieved by analyzing data from the essential services cluster. A summary of this analysis is reported in Figure 3. For each of the identified areas, we discusses some primary studies that we selected as illustrative examples.

3.1. *Sector*

Identifying essential service sectors for digital twin development is a critical step in enhancing community resilience and operational efficiency. Our analysis categorizes these sectors into five groups: utility management, infrastructure and transportation services, sector-wide essential services, urban and environmental systems, and community and societal services. These categories were derived from a total of 24 sources, including six peer-reviewed publications.

Utility management. In this category we find six sources, including one peer-reviewed publication. It focuses on ensuring reliable delivery and resilience of water, electricity, and gas services through maintenance, supply chain optimization, and sustainable practices [P5, G17].

Infrastructure and transportation services. In this category we find eight sources, including four peer-reviewed publications. It addresses the development and management of critical infrastructure, including roads, bridges, rail systems, and public transit [P6, P11]. These systems enable connectivity and societal functionality.

Critical services for public welfare. In this category we find six sources, including one peer-reviewed publication. It encompasses healthcare, education, emergency response, and industrial operations [**?** P3]. These services are critical for public health, safety, and welfare.

Urban and environmental systems. In this category we find three sources, including one peer-reviewed publication. It support sustainable development and environmental stewardship through urban planning and ecological monitoring [P3**?**].

Community and societal services. In this category we find three sources, including one peer-reviewed publication. It enhances social cohesion through welfare programs, community development, and recreational activities, fostering inclusion and engagement [**?**].

3.2. Evaluation methodology

The methodology for evaluating essential services is key to ensuring their efficiency, resilience, and adaptability. It is structured into four main categories: risk evaluation and management, data-driven decision making, urban and infrastructure planning, and optimization and monitoring. These categories were derived from a total of 18 sources, including seven peer-reviewed publications.

Risk evaluation and management. In this category we find five sources, including four peer-reviewed publications. It focuses on identifying, assessing, and mitigating risks to essential services. Key activities include risk quantification, threat modeling, contingency planning, and cybersecurity measures [P1, P8, P9], ensuring continuity and security.

Data-driven decision making. In this category we find three peer-reviewed sources. It leverages data analytics and information systems to improve service management. Processes like participatory observation, innovative data management solutions [P4], and transportation asset management [P10] enhance transparency, accountability, and operational efficiency.

Urban and infrastructure planning. In this category we find seven gray sources. It supports sustainable growth through land use, transportation, and infrastructure planning. Sub-categories such as socio-economic impact assessments [G17], city systems management, and grid resilience [?] ensure robust and adaptable urban environments.

Optimization and monitoring. In this category we find five gray sources. It involves the continuous improvement of essential services through performance metrics, quality control, and technological enhancements [G13]. Processes like simulation, evaluation, and performance monitoring [G15] ensure services operate efficiently and adapt to changing needs.

3.3. Societal impact

The societal impact of digital twins in essential services is significant, and can be categorized into three key areas: resilience and security, quality of life and sustainability, and equitable and informed access. These categories were derived from a total of 12 sources, including four peer-reviewed publications.

Resilience and security. In this category we find nine sources, including two peer-reviewed publications. It focuses on strengthening communities and infrastructure to recover from disruptions. Examples include infrastructure resilience to maintain energy and water systems during crises [G15], community safety initiatives to protect against cyber threats [P2], and ensuring reliable supply chains for essential goods [?].

5

Quality of life and sustainability. In this category we find five sources, including two peer-reviewed publications. It aims to improve well-being through sustainable practices. This includes integrating green technologies in urban planning [G12], promoting community health and happiness [P3], and prioritizing sustainable decision-making in infrastructure projects [?].

Equitable and informed access. In this category we find three sources, including two peer-reviewed publications. It ensures fair access to essential services like healthcare and education. For example, it includes addressing risks to equitable service delivery [P8], ensuring universal access to critical resources, and supporting underserved communities through targeted initiatives.

3.4. Interdependencies

Understanding and managing interdependencies within critical infrastructures is vital for systemic resilience and operational continuity. This approach can be categorized into three areas: critical infrastructure interactions, integrated planning and management, and technological enhancements for resilience. These categories were derived from a total of nine sources, including two peer-reviewed publications.

Critical infrastructure interactions. In this category we find three sources, including two peer-reviewed publications. It addresses the dependencies between sectors like energy, water, transportation, and telecommunications. It focuses on mitigating cascading effects from sector failures, managing cyber-physical attack scenarios [P1, P2], and implementing integrated alert systems for coordinated emergency responses [?].

Integrated planning and management. In this category we find three gray source. It emphasizes synchronizing planning and management across interdependent systems to enhance functionality and efficiency. Key aspects include resource and urban planning integration [G12], holistic urban planning using digital twins [G16], and preparedness for disasters to ensure effective emergency response [?].

Technological enhancements for resilience. In this category we find four gray sources. It leverages tools like digital twins, IoT, AI, and ML to predict, monitor, and manage complex interdependent systems. Examples include advanced disaster response technologies [?], sustainable infrastructure development [?], and digital twin integration to model system interdependencies [?].

3.5. Case study

Case studies on the application of digital twins in essential services offer valuable insights into their practical benefits across diverse sectors. These are categorized into six areas derived from a total of seven sources, including two peer-reviewed publications.

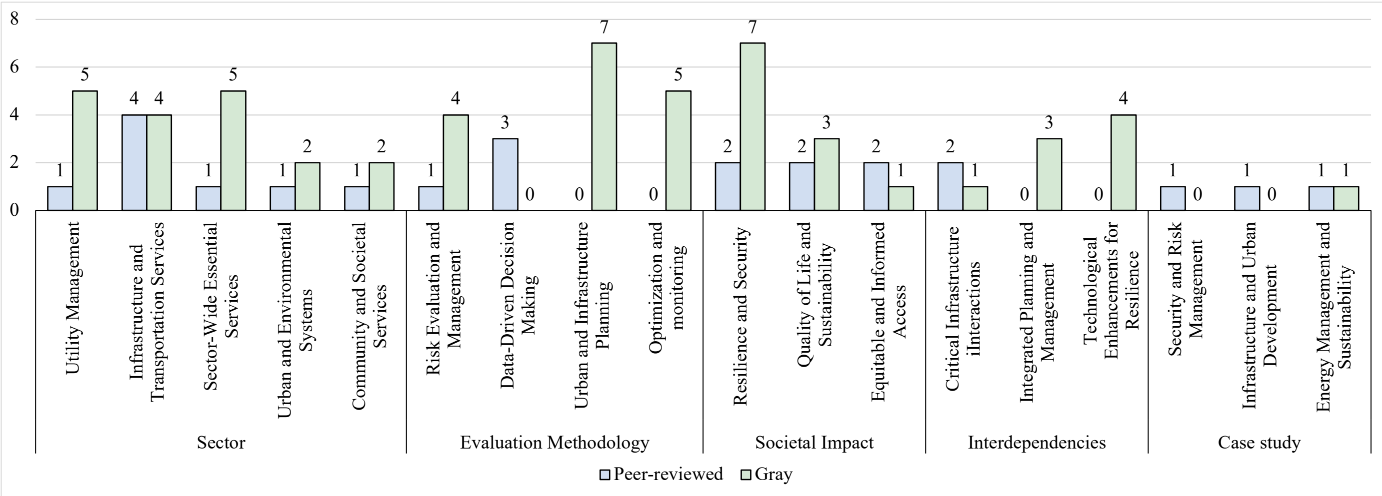

Figure 3: Distribution of peer-reviewed and gray literature sources across identified clusters and categories for RQ1.

Security and risk management. This area involves one peer-reviewed source and explores how organizations implement proactive strategies to safeguard assets, manage risks, and comply with regulations [P2]. Examples highlight the role of risk management and security protocols in protecting infrastructure and information.

Infrastructure and urban development. This area involves one peer-reviewed source and focuses on building resilient urban spaces, improving transportation networks, and enhancing public amenities through innovative planning and engineering [P3].

Energy management and sustainability. This area involves one peer-reviewed source and one gray source and showcases initiatives to optimize energy use, integrate renewable sources, and reduce carbon footprints, helping organizations meet environmental goals [P3, G15].

Digital twin implementation for planning and monitoring. This area involves three gray sources and highlights the use of digital replicas to simulate, monitor, and optimize operations in real time, improving decision-making and efficiency [G16, G18].

Industrial optimization. This area involves one gray source and demonstrates how industries leverage digital twins for automation to improve productivity, quality control, and cost-efficiency, particularly in contexts such as logistics centers [?].

Large-scale energy infrastructure management. This area involves one gray source and highlights. It examines strategies for managing power generation, transmission, and distribution systems to ensure reliability, efficiency, and sustainability [G15].

3.6. Contribution to resilience

DTs can improve societal resilience across three aspects: advanced technological resilience, infrastructure and operational resilience, and societal resilience and community support. These aspects are derived from a total of 22 sources, including seven peer-reviewed publications.

Advanced technological resilience. This aspect involves of seven sources, including six peer-reviewed publications and leverages cutting-edge technologies to predict, detect, and manage disruptions. Key elements include enhancing cybersecurity [P4, P5], AI-driven predictive analytics for maintenance and decision-making [P6, P7], and using digital twins to simulate and mitigate risks before they impact operations [?].

Infrastructure and operational resilience. This aspect involves of 11 sources, including two peer-reviewed publications and strengthens physical and operational systems to withstand and recover from crises. DTs enhance infrastructure durability and flexibility, supporting continuity in utilities, transportation, and public facilities [? ? ?]. They also aid in crisis recovery, sustainability efforts [P3], and investigating incident consequences across domains [P8].

Societal resilience and community support. This aspect involves four gray source and focuses on empowering communities through social cohesion, public health, and inclusive policies. DTs can enhance urban living quality by visualizing development plans and providing personalized information systems for residents and tourists [?]. Additionally, ensuring inclusivity for vulnerable groups is critical to a fair digital twin transition [G17].

Highlights – RQ1 As illustrated in Figure 3, DTs are most amenable to development in sectors essential for societal resilience, operational efficiency, and sustainability. These include:

- Utility management: enhancing reliability, maintenance, and resilience of water, electricity, and gas services through smart technologies and real-time monitoring [P4, P1, P5].
- Infrastructure and transportation services: optimizing roads, bridges, rail systems, and public transit for improved planning, monitoring, and connectivity [P6, P11].
- Sector-wide essential services: supporting healthcare, education, emergency response, and industrial operations with better service delivery, resource allocation, and safety[**?** P3].
- Urban and environmental systems: facilitating sustainable urban planning, environmental monitoring, and resource management for growth and conservation [G17**?**].
- Communications and energy systems: improving adaptability, efficiency, and sustainability of communication networks and energy infrastructure while addressing cyber-security challenges [G15**? ?** , G13].
- Industrial operations: enhancing production efficiency, quality control, and resilience in manufacturing, logistics, and agriculture, with applications extending to critical sectors like food and pharmaceuticals[**?** P3].

4. Role of safety-critical data requirements (RQ2)

In this section, we assess the role of data in safety-critical systems, addressing RQ2. Safety-critical systems are those whose failure can lead to catastrophic consequences, including threats to human life, damage to critical assets, or environmental harm. Therefore, securing and managing the data used by these systems is of paramount importance. To answer RQ2, we analyze data from the safety-critical data cluster and the results are summarized in in Figure 4. For each of the identified areas, we discusses some primary studies that we selected as illustrative examples.

4.1. Safety-critical data requirement

The actions required to assess safety-critical data can be grouped into three categories: real-time monitoring and management, threat detection and impact analysis, and data security and privacy. These categories were derived from a total of six sources, including five peer-reviewed publications.

Real-time monitoring and management. In this category we find two peer-reviewed sources. It ensures continuous oversight and control of safety-critical systems using real-time data [P1, P2]. This involves technologies that enable instant data acquisition, processing, and response, allowing immediate corrective actions for anomalies or potential threats. Key components include continuous performance monitoring [P1] and threat monitoring [P2].

Threat detection and impact analysis. In this category we find two peer-reviewed publications. It focuses on identifying potential threats and analyzing their effects on system stability and safety [P2, P4]. It utilizes advanced analytics, predictive modeling, and scenario simulations to preemptively address vulnerabilities and assess risks. Key aspects include comprehensive threat detection [P2] and specific threat analysis [P4].

Data security and privacy. In this category we find three sources, including two peer-reviewed publications. It protects critical data against unauthorized access or breaches [P7, P8]. Strategies include securing data at rest, in transit, and during processing, ensuring confidentiality, integrity, and compliance with privacy regulations. Key measures include data protection, privacy safeguards [P7], and digital twin security [**?**].

4.2. Safety-critical data assessment strategy

Defining strategies for assessing data in safety-critical systems is essential for minimizing the impact of faults and failures. Based on the literature reviewed, three key strategies have been identified: advanced threat simulation and resilience assessment, threat dynamics and propagation analysis, and anomaly detection with ML. These strategies were derived from a total of three peer-reviewed sources.

Advanced threat simulation and resilience assessment. In this strategy we find one peer-reviewed publication. It uses simulation tools to model potential threats and evaluate system resilience [P1]. Scenarios are created to predict system behavior under adverse conditions, identify vulnerabilities, and develop recovery plans. Key components include simulation tools, impact modeling, and real-time resilience metrics [P1].

Threat dynamics and propagation analysis. In this strategy we find one peer-reviewed publication. It examines how threats evolve and spread within or across systems [P2]. It focuses on understanding threat behaviors, conditions that enable escalation, and pathways for potential impacts, providing insights for containment and mitigation strategies.

Anomaly detection with ML. In this strategy we find one peer-reviewed publication. It applies AI techniques to identify deviations from normal operations [P4]. Algorithms trained on typical system behavior detect anomalies in real-time data streams, enabling early intervention to prevent security breaches or failures.

4.3. Data security measures

Data security technologies and solutions must detect, monitor, and respond to diverse threats at multiple levels, ensuring comprehensive data protection. The literature identifies four categories of solutions for data security, integrity, and access: threat detection and awareness, adaptive security measures, technological implementations for security, and comprehensive cybersecurity strategies. These strategies were derived from a total of six sources, including five peer-reviewed publications.

Threat detection and awareness. In this strategy we find two peer-reviewed publications. It focuses on identifying and monitoring potential security threats [P1, P2]. It involves systems that continuously scan for anomalies or vulnerabilities, using real-time monitoring and alerting mechanisms to promptly address potential risks.

Adaptive security measures. In this strategy we find one peer-reviewed publication. It emphasizes dynamic responses to evolving threats and vulnerabilities [P1]. These solutions adjust security protocols based on user behavior and network conditions, ensuring effectiveness as new threats emerge and digital infrastructure changes.

Technological implementations for security. In this strategy we find one peer-reviewed publication. It covers advanced tools like encryption, firewalls, and intrusion detection systems [P11]. These technologies protect data integrity and confidentiality, providing a critical line of defense against external attacks and breaches.

Comprehensive cybersecurity strategies. In this category we find three sources, including two peer-reviewed publications. It involve system-wide protocols that govern data access, authentication, network security, and incident response [P6, P8]. These overarching strategies create a secure, resilient infrastructure by protecting all facets of an organization's digital and physical operations.

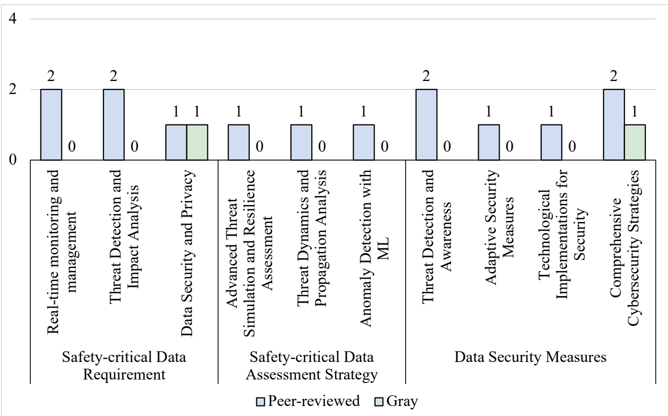

Figure 4: Distribution of peer-reviewed and gray literature sources across identified clusters and categories for RQ2.

Highlights – RQ2 As summarized in Figure 4, safety-critical data plays a central role in the development and maintenance of DTs, underpinning their functionality, reliability, and security.:

- Operational integrity: real-time monitoring and management provide accurate, up-to-date insights, enabling immediate responses to anomalies and supporting system continuity [P1, P2].
- Risk mitigation: data enables risk assessment through threat detection and predictive modeling, helping prevent failures and build resilient systems [P2, P4].
- Security and privacy: advanced technologies like encryption and adaptive protocols safeguard data integrity and maintain system reliability [P11, P7].
- Adaptive resilience: safety-critical data supports DTs in adapting to evolving threats, enhancing long-term resilience and effectiveness [P1].
- Simulation and prediction: data powers simulations to predict behavior, assess resilience, and guide decision-making for optimized system performance [P1].

5. Use of DTs for identifying, evaluating, and mitigating risks within essential services (RQ3)

In this section, we explore how DTs can identify, evaluate, and mitigate risks within essential services, addressing RQ3. This is achieved by analyzing data from the risk identification and mitigation, SoS, and AI/ML clusters. A summary of this analysis is reported in Figure 5. For each of the identified areas, we discusses some primary studies that we selected as illustrative examples.

5.1. Risk identification techniques

We focus on essential DT components, including simulation and analytics, that are critical for risk identification. The literature identifies four categories: advanced risk analysis and simulation, surveillance and behavior analytics, cybersecurity and threat mitigation, and predictive maintenance and operational resilience. These categories were derived from a total of four peer-reviewed publications.

Advanced risk analysis and simulation. In this strategy we find one peer-reviewed publication. It uses analytical models and simulation tools to assess potential risks and their impacts [P1]. Detailed scenario simulations enable organizations to foresee outcomes and implement mitigation strategies. Literature explores quantitative risk assessment, system simulations, and DT applications in risk management.

Surveillance and behavior analytics. In this strategy we find one peer-reviewed publication. It focuses on monitoring and analyzing system behaviors to detect anomalies or security threats [P2]. Advanced analytics tools interpret data patterns, allowing for early detection of risks and swift responses to maintain security and integrity.

Cybersecurity and threat mitigation. In this strategy we find one peer-reviewed publication. It encompasses strategies and technologies to protect systems from cyber threats [P4]. This includes firewalls, antivirus software, and advanced cybersecurity frameworks to prevent unauthorized access, data breaches, and cyber attacks.

Predictive maintenance and operational resilience. In this strategy we find one peer-reviewed publication. It utilizes predictive analytics to anticipate failures and schedule maintenance proactively [P6]. By monitoring infrastructure and equipment, organizations can minimize downtime, optimize maintenance schedules, and ensure operational continuity.

5.2. Risk mitigation strategies

In the literature, three main categories of strategies have been identified for leveraging DTs in risk management while minimizing potential drawbacks: advanced technological integration in risk management, predictive maintenance and system optimization, and comprehensive disaster preparedness and response planning. These categories were derived from a total of 10 sources, including four peer-reviewed publications.

Advanced technological integration in risk management. In this category we find three peer-reviewed sources. It focuses on applying cutting-edge technologies like AI, ML, big data analytics, and IoT to enhance risk management processes [P1, P2, P8]. By automating and improving the detection, analysis, and mitigation of risks, these technologies enable rapid and effective responses to potential threats, reducing vulnerabilities and enhancing security. Key aspects include security orchestration and automated responses [P1, P2, P11], as well as AI-driven adaptation and response capabilities [P1, P11].

Predictive maintenance and system optimization. In this category we find four sources, including one peer-reviewed publication. It uses predictive analytics and data-driven approaches to anticipate and prevent system failures [P6, G15? ?]. This approach leverages historical data and real-time insights to forecast maintenance needs, reducing downtime and optimizing system performance and lifespan. Activities include continuous monitoring, predictive maintenance [P9, G15], and proactive system adaptations [G15? ?].

Comprehensive disaster preparedness and response planning. In this category we find three gray sources. It involves creating detailed plans and protocols for disaster readiness and recovery, addressing both natural and man-made crises [G12? ?]. This includes strategic planning, resource allocation, training, and simulation exercises to ensure operational continuity during a crisis and rapid recovery afterward. Critical elements include digital twin-enabled scenario simulation and resilient infrastructure design and testing.

5.3. Relevance of DTs in SoS

Many societal systems are formed by interconnecting technical and organizational systems that are owned and operated by independent companies or public authorities. This makes the SoS concept relevant to societally critical systems, and the literature identifies four aspects: system configuration and operational adaptability, strategic disruption management and resilience planning, comprehensive integration and monitoring systems, and advanced data management and sectoral applications. These aspects were derived from a total of 12 sources, including four peer-reviewed publications.

System configuration and operational adaptability. In this aspect we find two peer-reviewed publications. It emphasizes the flexibility of digital twins in dynamically adapting to changing conditions within complex systems. This adaptability enhances operational efficiency and effectiveness. Mathur discusses a modular DT architecture enabling flexibility across applications [P5], while Lampropoulos and Siakas explore DTs in Industry 4.0 and IIoT, identifying them as service architectures for cyber-physical systems, with challenges relevant to societally critical systems [P7].

Strategic disruption management and resilience planning. In this category we find four sources, including two peer-reviewed publications. It involves using DTs to simulate and manage disruption scenarios, enabling resilience strategies to mitigate risks. Rios et al. highlight DTs as key to managing interconnected critical infrastructures [P1], while Schauer et al. propose a framework integrating physical and cyber DTs for comprehensive resilience management [P8]. Sharp extends this concept to national-scale DTs for disaster response planning [G13], with applications in urban planning for evaluating designs [?].

Comprehensive integration and monitoring systems. In this category we find four gray source. It describes DTs as platforms for real-time data collection, analysis, and visualization across subsystems in an SoS. This integration ensures system-wide stability and performance. Examples include DT applications in smart cities for urban and environmental system integration [G16?], water infrastructure management [?], and distributed industrial and public infrastructure [?].

Advanced data management and sectoral applications. In this category we find two gray source. It focuses on using DTs for tailored data management and decision-making in sectors like manufacturing, healthcare, and urban planning. DTs enable precise process optimization and improved outcomes, such as supply chain dashboards or "national control towers" [?], and water infrastructure interconnectivity [?].

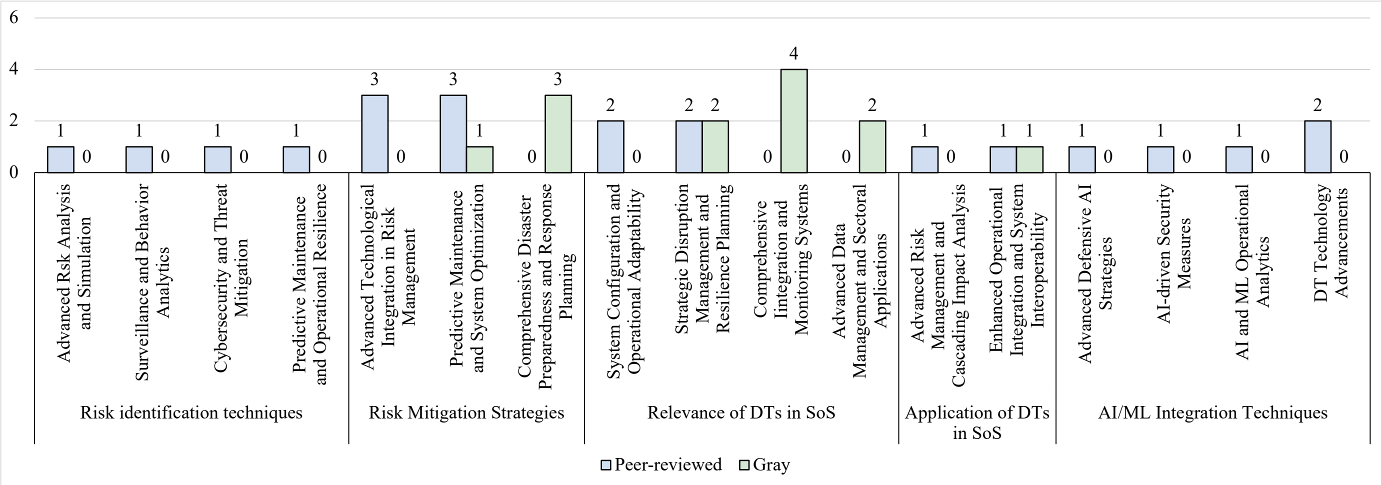

Figure 5: Distribution of peer-reviewed and gray literature sources across identified clusters and categories for RQ3.

5.4. Application of DTs in SoS

In the context of SoS applications, two key categories of DT use have been identified: advanced risk management and cascading impact analysis, as well as enhanced operational integration and system interoperability. These categories were derived from a total of three sources, including two peer-reviewed publications.

Advanced risk management and cascading impact analysis. In this category we find one peer-reviewed publication. It leverages digital twins to conduct in-depth risk assessments and analyze how disruptions in one part of the system can propagate to others. By simulating various scenarios, DTs help organizations understand interdependencies, predict cascading impacts, and develop strategies to mitigate risks effectively. Rios et al. propose a framework for critical infrastructure and cybersecurity, enabling information propagation to infrastructure operators for risk assessments and incident reporting [P1].

Enhanced operational integration and system interoperability. In this category we find two sources, including one peer-reviewed publication. It focuses on improving coordination and cohesion among constituent systems in an SoS. DTs act as a unifying platform, synchronizing operations across disparate systems and technologies, thereby enhancing system efficiency and responsiveness. Examples include integrating technical 3D infrastructure models with sensory data [?] and using DTs for situational awareness in complex scenarios, such as mitigating a terrorist attack at an airport based on sensory systems coordination [P2]. These applications demonstrate the critical role of interoperability in ensuring effective system-wide performance and management.

5.5. AI/ML integration techniques

The integration of AI and ML is transforming efficiency, security, and operational management across sectors. This transformation can be categorized into four key areas: advanced defensive AI strategies, AI-driven security measures, AI and ML operational analytics, and digital twin technology advancements. These areas were derived from a total of five sources, including two peer-reviewed publications.

Advanced defensive AI strategies. In this area we find one peer-reviewed publication. It uses adaptive intelligence techniques (e.g., deep-learning–driven anomaly detection, threat simulation, probabilistic risk modeling, reinforcement-learning–based orchestration, SDN-driven self-healing, and automated CTI sharing) to enhance system security [P1]. These AI systems autonomously detect, analyze, and respond to potential threats and anomalies, learning and adapting from incidents to proactively mitigate risks. By evolving in response to new challenges, these strategies strengthen the security posture of organizations.

AI-driven security measures. In this area we find one peer-reviewed publication. It applies ML models (e.g., anomaly classifiers, deep-learning feature extractors, statistical forecasters, and RL-driven orchestrators) to monitor, detect, and respond to cyber threats in real-time [P4]. Leveraging data analytics and scalable streaming, these measures improve threat detection accuracy, streamline security protocols, and automate responses to repetitive threats, enhancing responsiveness and effectiveness.

AI and ML operational analytics. In this area we find one gray source. It optimizes processes by analyzing operational data with predictive models (e.g., simulation-optimization, AI/ML-driven analytics) and data-driven insights [G16]. This application improves decision-making, operational efficiency, and trend forecasting, turning large datasets into actionable intelligence that drives organizational improvements.

DT technology advancements. In this area we find two gray sources. It integrates computer-vision–driven 3D reality capture and AI-powered inventory reconciliation (linking drawings to as-built scans), along with machine-learning anomaly detectors, time-series forecasting models, and optimization-based simulation in its digital twins [? ?]. This combination sharpens real-time monitoring, predictive maintenance, and what-if analyses, enabling smarter operations and faster innovation in complex infrastructures.

Highlights – RQ3 As summarized in Figure 5,, DTs play a key role in managing risks within essential services by leveraging advanced analytics, system integration, and AI-driven capabilities to enhance resilience and efficiency:

- Risk identification: DTs use simulation tools, real-time analytics, and surveillance systems to detect risks and anomalies. Scenario simulations foresee risks [P1], surveillance tools enable early threat detection [P2], and predictive analytics optimize maintenance [P6].
- Risk mitigation: DTs integrate AI, IoT, and big data to automate risk detection and response [P1]. Predictive maintenance ensures performance [G15], while scenario simulations support disaster planning [?].
- SoS integration: DTs improve stability and functionality across interconnected systems by simulating cascading impacts [P1] and enhancing interoperability for seamless operations [P2].
- AI/ML integration: AI and ML enhance DTs with adaptive intelligence and predictive analytics. AI systems detect and respond to threats [P1], while operational analytics improve decision-making [G16].

6. Discussion

Building on the analysis presented in the previous sections, we now discuss several cross-cutting issues, integrating our findings with practitioners' insights gathered during the interviews. These insights are marked with a capital 'I', following the notation introduced in Section 2. These relate to the definition of DTs, how DTs differ from other related concepts, and some of the key challenges of introducing DTs in essential services in society.

6.1. What is a DT?

Through our study, we identified 22 different DT definitions, highlighting the absence of a unified understanding in the research community. Despite these variations, several commonalities emerged.

DTs are consistently described as digital models or replicas of physical entities, processes, or systems. A key feature is their dynamic connection to their physical counterparts, often achieved through real-time or near-real-time data integration. This connection ensures that DTs accurately reflect the current state of the physical system, enabling monitoring, simulation, and optimization. DTs are recognized for their versatility and applicability across various domains, including manufacturing, infrastructure, energy systems, and urban planning. They serve as tools to enhance understanding, optimize operations, and enable predictive analytics. For instance, Rios et al. describe DTs as virtual models that integrate real-time situational awareness to enable simulations and interconnections [P1], while Sousa et al. highlight their ability to mirror physical systems accurately for security analysis and risk evaluation [P4].

However, the definitions also exhibit notable differences, reflecting the diverse applications and priorities within various industries. In manufacturing, DTs are often framed as enablers of smart production within Industry 4.0, where they bridge the physical and virtual worlds to address challenges associated with digitization [P7]. In contrast, definitions related to infrastructure and energy systems focus on their role in enhancing grid operations, optimizing maintenance, and improving resilience [G15]. Urban planning definitions emphasize their use in disaster-resilient infrastructure development and scenario simulations [?]. The scope of data integration also varies significantly. Some definitions emphasize simple sensor-based updates, while others incorporate complex systems such as SCADA and IoT for continuous feedback and control [? ?]. Similarly, the functionality of DTs is portrayed differently, ranging from tools for real-time monitoring to platforms for collaborative decision-making and scenario testing [? G16].

6.2. Difference with related concepts

DTs represent a significant evolution from traditional models and simulations, offering unique capabilities that distinguish them in both technical and practical applications. Unlike conventional approaches, DTs integrate advanced technological features, deliver operational enhancements, and provide strategic advantages that redefine how systems and processes are designed, monitored, and managed.

One of the key distinctions of DTs lies in their technical advantages. Unlike static models or isolated simulations, DTs are dynamic, real-time systems capable of high fidelity and seamless inter-connectivity with IoT platforms. These attributes allow DTs to provide precise and continuously updated representations of physical assets. Their predictive capabilities enable foresight into potential issues, while qualities such as configurability, accessibility, and plugin integration enhance their adaptability and usability [P1, P2]. Additionally, DTs support multiple operational modes, further distinguishing them from traditional static models [P2].

DTs also offer notable operational benefits (I2, I3), enabling substantial improvements in the efficiency and reliability of day-to-day processes. Through real-time data insights, DTs enhance decision-making by providing actionable intelligence that supports predictive maintenance, reduces downtime, and minimizes operational risks. They enable the safe simulation and testing of scenarios without impacting physical systems, leading to cost savings and increased safety. Examples include advancements in intelligent manufacturing and data management, where DTs streamline decision-making processes and optimize operations [P7, P8, P10].

The strategic utility of DTs further sets them apart by enabling organizations to conduct comprehensive risk analysis and foster innovation. DTs provide environments for safely testing new strategies, technologies, or upgrades without disrupting actual operations, making them invaluable for long-term planning and adaptation. By offering a holistic overview of system inter-dependencies, DTs help manage complexity and support sustainable growth [? ?]. Their ability to facilitate safe implementation and upgrades ensures that organizations can evolve and remain competitive in dynamic environments [?].

6.3. Challenges of using DTs for essential services

Implementing DTs, especially for essential services, is still in the early stages of development, as indicated by the relatively few publications in the field. There are many challenges that need to be addressed. These challenges stem both from DTs themselves and from the relevant technologies, particularly those arising due to their complex and interconnected nature, trustworthiness, high cost, and investment (I1, I2, I3).

Complexity. DTs for essential services are complex systems due to the following:

- *Managing multiple complex and dependable models.* Models in DTs for essential services include not only the models that will optimize diverse functionalities of these services, but also many other supporting models (I1), for example, models that assure cyber-security protection [?]. A failure in a model might have a significant impact on other models due to the complexity and interdependency among them [P1].
- *ML-based models.* Many of the models that would be used for essential services are ML-based models needed to capture the complex behavior of physical assets. Many such models require big data to be trained and should be updated dynamically during run-time.
- *Customization.* Proposed DT solutions for essential services need to be customized based on specific requirements and consider application-specific issues critical from safety, security, time or business perspectives. Hence, there is no single solution that fits all needs for essential services. In addition, the market offers many commercial solutions with difficulties in validating their suitability without substantial investigation [P5]
- *Domain knowledge.* A wide range of domain knowledge is needed since DTs for essential services involve multiple dimensions, including protecting physical processes, communication and computation infrastructure, and managing the life-cycle of hardware and software. These aspects require a domain-specific approach rather than standard IT strategies [P8].
- *Distributed decision-making.* Most essential services require collaboration between several independent organizations, which all have their own goals and interests (I1). To make such a system of systems situation work, mechanisms are needed that provide incentives and infrastructure for aligning the efforts and decisions towards the societal interest.

Trustworthiness and reliability. Since essential services involve systems with complex behavior, ML models are the most suitable solution for modeling such systems and making smart and efficient decisions. Thus, the correctness of the results, securing models, and complying with policies and procedures become extremely important aspects (I3).

- *Accuracy of results.* The accuracy of the results generated by ML models depends on the quality and relevance of the training data, their correctness, training methods, and the size and representation of data. This means that the results generated might not be correct, which might affect the performance of DT. This might affect the cyber-security if the models used to protect DTs are not accurate/efficient.
- *Security of models.* Because ML models rely on extensive data, it is important to ensure their protection as they can become significantly powerful and could provide details of information which might not be possible to obtain from some data. These models can be vulnerable to security violations like data breaches and will be targets for attacks [P8].
- *Compliance.* The use of AI needs to comply with national and international regulations. One scenario could be if the data used to train models or make decisions contains personal information, then permission from the persons should be obtained before it is used which is not always easy. In addition, the development of AI-based solutions, especially for essential services as it may contain sensitive information, should follow national and international regulations. An example is the EU legal framework called AI Act that fosters trustworthy AI in Europe by assessing the risk of using such services for each case[4].

Investments. Implementing DTs for essential services requires significant investments in financial resources, infrastructure, and staff competencies. Investment areas include:

- *Infrastructure.* Creating infrastructure suitable for implementing DTs for essential services requires substantial investment in hardware and software (I1, I2, I3). Running DTs in such applications requires efficient collection, management, and extraction of information and knowledge from big data, training AI models,

[4]https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

running simulation models continuously, and making smart and optimal decisions in real-time. This requires strong computation, efficient computer networks, and high storage capacity [P10].

- *Skills and competencies.* Excellent skills in IT, data science, and cyber-security are required. Competencies in managing the transition to DTs and boosting the digital skills of regular staff members are also necessary [P10].

7. Related work

To the best of our knowledge, this study represents the first peer-reviewed mixed-methods research examining the potential of DTs in essential services, combining insights from systematic literature reviews, gray literature, and expert interviews.

As illustrated in Figure 6[5], interest in DTs has grown significantly in recent years, leading to a body of work, many included in our study, exploring innovative applications of DT in essential services. For example, Rios et al. [P1] discuss the use of DTs for dynamic risk management and situational awareness in critical infrastructure, emphasizing their ability to simulate cascading effects and inform decision-making during crises. Similarly, Sousa et al. [P4] highlight DTs' potential in improving operational efficiency and security in aviation, demonstrating how real-time data integration can enhance resilience and risk mitigation strategies. Additionally, a significant body of systematic literature reviews has emerged, reflecting the growing importance of DTs across various fields. These reviews span disciplines such as software engineering, production, and manufacturing, providing valuable insights into different aspects of DT technology. For instance, Ferko et al. systematically reviewed architectural concerns related to DTs, offering an in-depth analysis of how DT architectures are designed and implemented [?]. Similarly, Liu et al. conducted a comprehensive review of DT concepts, technologies, and industrial applications, highlighting their transformative impact in sectors like manufacturing and logistics [?] . While these reviews provide foundational knowledge and insights, they are complementary to our work, as they do not focus on the specific applications of DTs in essential services.

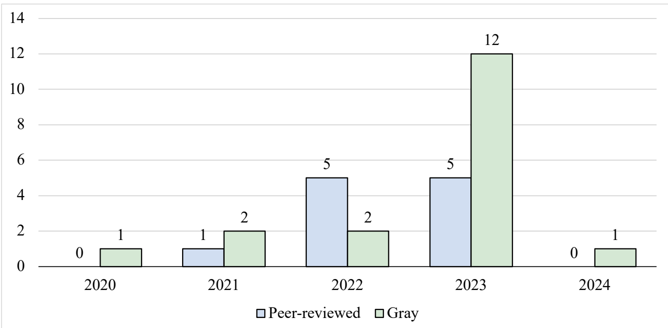

Figure 6: Temporal distribution of selected studies on digital twins in essential services.

In the context of infrastructure management, Nandhakumar [G12] explores the role of DTs in optimizing power generation and distribution systems, showcasing their capacity to enhance maintenance strategies and support sustainable energy transitions. Moreover, urban planning and environmental management have also seen promising applications, as described by urbanCGI [?], which illustrates how DTs can aid in disaster-resilient infrastructure design and scenario testing for urban environments.

While existing studies and reviews underscore the transformative potential of DTs, most focus on specific sectors, theoretical models, or experimental applications, often lacking a comprehensive view of their applicability across the diverse spectrum of essential services. Our mixed-methods approach bridges this gap by synthesizing existing knowledge and incorporating insights from practitioners, offering a more holistic understanding of how DTs can be effectively leveraged in societal critical applications.

This study not only extends the existing body of knowledge, but also offers actionable recommendations for stakeholders, including policymakers and industry leaders.

8. Conclusions and recommendations

DTs are increasingly becoming standard practice across domains like manufacturing and process industries, propelled by technological advancements and ongoing standardization efforts. The integration of AI and machine learning enhances their capabilities, unlocking new opportunities for efficiency, resilience, and innovation. This study consolidated the existing knowledge on DT applications in sectors critical to societal functioning. Using a systematic review of both academic literature and gray sources, complemented by expert interviews, it captured insights from both the state of the art and the state of practice.

8.1. Summary of key findings

The literature highlights several significant benefits of employing DTs in sectors critical to societal functioning.

Enhanced crisis preparedness. DTs improve situational awareness and crisis management by enabling high-fidelity, real-time simulations of essential services, supporting more effective emergency response.

Operational efficiency. Continuous monitoring and predictive maintenance capabilities allow DTs to enhance the operational efficiency and safety of critical infrastructures.

[5]It should be noted that the low number of studies for 2024 is due to the automatic search being conducted within the first three months of the year.

Strategic planning. Real-time data integration supports robust strategic planning, enabling organizations to anticipate and adapt to potential disruptions effectively.

Interoperability and collaboration. DTs foster better coordination among stakeholders managing essential services, leading to more unified and efficient response strategies during emergencies.

Despite these potential benefits, the field remains in its exploratory phase, with limited real-world experiences and applications documented. While the optimistic projections of DT capabilities are promising, they must be tempered with an awareness of the costs and complexities associated with large-scale implementation—an area that remains under-explored in the current literature.

8.2. Actionable recommendations for private sector and industry

The potential of DTs, as highlighted in the literature, suggests a growing interest among organizations to harness their benefits. In addition, many operations that are critical to society are carried out by private companies, and the private industry is also the supplier of the technology for DTs. Therefore, the symbiosis between public and private actors is essential. To maximize the effectiveness and adoption of DT technologies, the following actions are recommended.

Invest in DT technologies. Support the adoption of DTs to improve operational resilience and enhance capabilities in crisis response and resource management.

Prioritize data security. Ensure the security, integrity, and accessibility of data within DTs to maintain trust and reliability, particularly in safety-critical applications.

Develop standardized protocols. Establish protocols for data sharing and system integration to promote interoperability and efficiency across diverse DT platforms and applications.

Evaluate life-cycle costs and benefits. Recognize DTs as complex IT systems requiring ongoing investment. Conduct thorough analyses of life-cycle costs, including upgrades and enhancements, to ensure sustained value and mitigate the high failure rate observed in digital transformation projects [**?**].

Collaboration with government. Engage in partnerships with government agencies to align DT development with national safety standards and requirements.

Innovation in DT applications. Innovate in the application of DTs beyond traditional uses, exploring new areas like sustainable urban planning and renewable energy management.

8.3. Implications for government agencies

Government agencies, such as Sweden's MSB, can undertake several actions to facilitate the sensible introduction of digital twins (DTs) in societally critical applications:

Policy development. Develop policies that encourage the integration of DTs into public safety and emergency management frameworks while regulating their use to mitigate potential downsides.

Preparation for DT introduction. Ensure that new assets are designed with real-time data access and machine-readable models to simplify later integration into DTs. Incorporate a SoS perspective to facilitate collaboration across public and private organizations managing interconnected assets.

Funding and research. Allocate dedicated funding to advance research and development of DT applications in public infrastructure and safety.

8.4. Future research directions

The literature reveals that the application of DTs to societally critical areas is still immature, and there is ample need for further investigations:

DTs in non-conventional areas. Explore the use of DTs in less traditional sectors such as renewable energy and smart cities.

Long-term impact studies. Conduct long-term studies to assess the societal and environmental impacts of DTs in essential services. This can lead to both scientifically sound evaluations of cost and benefits, and valuable accounts of practical experiences.

Advanced AI integration. Investigate advanced AI techniques to enhance the predictive capabilities and autonomy of DTs.

Cross-disciplinary research. Much of the existing literature has a focus on technology, and this is important to understand the building blocks of a DT. However, as the field matures, there is also a need for systems-oriented research that looks at the problems more broadly, and includes technology, organizations, people, and society.

SoS perspective. Societal applications fulfill many of the characteristics of SoS, but the literature on DTs in this sector hardly brings up this perspective at all. Further research is thus needed on how DTs can be used to improve the collaboration in a societal SoS, and how known hurdles can be overcome [**?**].

Acknowledgment

This research has been funded by the Swedish Civil Contingencies Agency (MSB) under grant no. 2023-14230, by the Swedish Knowledge Foundation through the MoDEV project (20200234), by Vinnova through the iSecure project (202301899), and by the KDT Joint Undertaking through the MATISSE project (101140216).

Appendix. Primary studies

[P1] E. Rios, E. Iturbe, A. Rego, N. Ferry, J.-Y. Tigli, S. Lavirotte, G. Rocher, P. Nguyen, H. Song, R. Dautov, et al., The dynabic approach to resilience of critical infrastructures, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–8.

[P2] S. Schauer, T. Hadjina, M. Damjanovic, E. M. Muñoz Navarro, J. J. Hernandez Montesinos, J. H. Gómez, L. Papadopoulos, Detecting a complex attack scenario in an airport: The praetorian framework, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–7.

[P3] L. Sarv, R.-M. Soe, Piloting smart city solutions in very small, small and medium-sized municipalities. the estonian case study, in: Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, 2022, pp. 475–482.

[P4] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço, T. Cruz, Elegant: Security of critical infrastructures with digital twins, IEEE Access 9 (2021) 107574–107588.

[P5] A. P. Mathur, Reconfigurable digital twin to support research, education, and training in the defense of critical infrastructure, IEEE Security & Privacy 21 (4) (2023) 51–60.

[P6] J. Vieira, J. Poças Martins, N. Marques de Almeida, H. Patrício, J. Gomes Morgado, Towards resilient and sustainable rail and road networks: A systematic literature review on digital twins, Sustainability 14 (12) (2022) 7060.

[P7] G. Lampropoulos, K. Siakas, Enhancing and securing cyber-physical systems and industry 4.0 through digital twins: A critical review, Journal of Software: Evolution and Process 35 (7) (2023) e2494.

[P8] S. Schauer, M. Latzenhofer, S. König, S. Chlup, C. Schmittner, Application of a generic digital twin for risk and resilience assessment in critical infrastructures, in: ESREL 22-32nd European Conference on Safety and Reliability, Dublin, Ireland, 2022, pp. 2765–2772.

[P9] C. Grasselli, A. Melis, L. Rinieri, D. Berardi, G. Gori, A. Al Sadi, An industrial network digital twin for enhanced security of cyber-physical systems, in: 2022 International Symposium on Networks, Computers and Communications (ISNCC), 2022, pp. 1–7.

[P10] A. Ammar, F. Maier, R. Catchings, H. Nassereddine, G. Dadi, Departments of transportation efforts to digitize ancillary transportation asset data: A step toward digital twins, Transportation Research Record 2677 (11) (2023) 428–445.

[P11] R. Dirnfeld, L. De Donato, A. Somma, M. S. Azari, S. Marrone, F. Flammini, V. Vittorini, Integrating ai and dts: Challenges and opportunities in railway maintenance application and beyond, Simulation (2024) 00375497241229756.

[G12] S. Nandhakumar, Revolutionising government services through digital twins: Unleashing innovation and efficiency, https://www.linkedin.com/pulse/revolutionising-government-services-through-digital-nandhakumar/, August 2023.

[G13] M. Sharp, The importance of digital twins for telecommunications and utilities, https://www.iqgeo.com/blog/the-importance-of-digital-twins-for-telecommunications-and-utilities, March 2022.

[G14] H. Kadia, The digital twin revolution — how businesses are using virtual models to optimize their operations, https://techknexus.com/5g-network/shaping-future-connectivity-tech-5g-magazine-may-2023/digital-twin-revolution-how-businesses-are-using-virtual-models-to-optimize-their-operations/, May 2023.

[G15] S. Nandhakumar, Enhancing power infrastructure with digital twins, https://www.linkedin.com/pulse/enhancing-power-infrastructure-digital-twins-sarawanan-nandhakumar/, September 2023.

[G16] Westcott Space Cluster, Digital twin showcase: What is a digital twin?, https://westcottspacecluster.org.uk/digital-twin-showcase-what-is-a-digital-twin/, April 2023.

[G17] European Commission, Access to essential services: Key challenges for the most vulnerable – report, https://ec.europa.eu/social/main.jsp?langId=en&catId=89&furtherNews=yes&newsId=105, June 2023.

[G18] Bable Smartcities, Discover the alternative barcelona, europe's first digital twin, https://www.bable-smartcities.eu/spot/posts/post/discover-the-alternative-barcelona-europes-first-digital-twin.html, 2024.

[] Vroc, The benefits of a city digital twin, https://vroc.ai/benefits-of-a-city-digital-twin/, accessed 2024.

[] S. Jagdale, Transforming industrial iot with digital twin integration, https://iot.eetimes.com/transforming-industrial-iot-with-digital-twin-integration/, June 2022.

[] SAMP, SUEZ and SAMP improve the resilience of water infrastructure, https://samp.ai/suez-and-samp-sign-a-partnership-to-improve-the-resilience-of-water-infrastructure-through-digital-twins/, October 2023.

[] VDE ETG, The digital twin in the network and electricity industry, https://www.vde.com/resource/blob/2293228/3e50b3417c8777c85e9e33cb3e1e9ebc/vde-st-a4-digital-twin-12-2023-final-data.pdf, May 2023.

[] S. Nolan, How singapore is future proofing its energy grid with digital twins, https://govinsider.asia/intl-en/article/how-singapore-is-future-proofing-its-energy-grid-with-digital-twins-jeanette-lim-energy-market-authority, April 2022.

[] PST CLC Mitsui-Soko, PST CLC Mitsui-Soko is preparing digital twins of its own logistics centres. the company will focus on digitalisation and process optimisation, https://pst-clc.com/pst-clc-mitsui-soko-is-preparing-digital-twins-of-its-own-logistics-centres-the-company-will-focus-on-digitalisation-and-process-optimisation/, August 2023.

[] LIST, A 'national control tower' monitoring and preventing collapse of essential services, https://www.list.lu/en/news/a-national-control-tower-monitoring-and-preventing-collapse-of-essential-services/, June 2020.

[] BaseN, Innovate on mission critical resilience, https://www.basen.net/innovate-on-mission-critical-resilience/, July 2023.

[] ESRI, Gwinnett county explores benefits of digital twins at pump station, https://www.esri.com/en-us/lg/industry/water/gcdwr-case-study, accessed 2024.

[] Urban CGI, Disaster-resilient infrastructure: The benefits of CGI digital twins, https://www.urbancgi.com/infrastructure-planning/disaster-resilient-infrastructure/, accessed 2024.

[] Globe Newswire, New digital twin consortium working group targets telecommunications, https://www.globenewswire.com/news-release/2023/03/20/2630323/0/en/New-Digital-Twin-Consortium-Working-Group-Targets-Telecommunications.html, March 2023.

[] T. Eliot, Digital advancements in water, https://smartwatermagazine.com/news/bentley-systems/digital-advancements-water, March 2021.

[] SAP, The digitalization behind australia's $140b critical infrastructure spend, https://news.sap.com/2021/11/digitalization-behind-australias-140b-critical-infrastructure-spend/, November 2021.

[] A. Camus, How a digital twin helped to modernise brazil's sanitation system, https://www.smartcitiesworld.net/dig

ital-twins/how-a-digital-twin-helped-to-modernise-brazils-sanitation-system, October 2023.

[] E. Thomas, Digital solutions for indonesia's ageing energy assets, https://www.energymonitor.ai/newsletters/digital-solutions-for-indonesias-ageing-energy-assets/, December 2023.