Enhancing Critical Infrastructure Resilience against Climate Crisis with Digital Technologies

Lin Dong
Department of Crisisonomy, Chungbuk National University, Cheongju, Korea

Abstract

This study aims to explore how integrating digital technologies, such as IoT, digital twins, AI, and BIM, can enhance infrastructure resilience against the increasing frequency and severity of extreme weather events due to climate change. These technologies provide real-time data, predictive maintenance, and improved decision-making capabilities. Traditional management methods are identified as fragmented and manual, highlighting the need for digital solutions. However, challenges such as cybersecurity risks, human-machine interaction conflicts, and funding barriers must be addressed. The study concludes with recommendations for adopting digital technologies to ensure infrastructure stability and promote sustainable development.

Keywords: Critical Infrastructure Resilience, Digital Technologies, Critical Infrastructure Asset Management, Climate Change

I. Introduction

Climate change is a severe challenge facing human society today. Global warming has intensified the frequency and severity of extreme weather events, posing significant challenges to critical infrastructure systems that ensure the normal functioning of society(Huddleston, *et. al.*, 2022). For example, during the 2015-2016 drought in Kenya, the lack of rain, high temperatures, and strong winds led to water shortages, power outages, and damage to public facilities(King-Okumu, *et. al.*, 2020). In 2018, Japan's Kansai International Airport, a crucial transportation hub, was forced to suspend operations because of Typhoon Jebi's strong winds and storm surges(Suzuki, *et. al.*, 2020). From 2019 to 2020, wildfires in Australia damaged power lines, leaving local communities without stable electricity(Ahmed & Ledger, 2023). In 2021, a winter storm in North America caused water pipes to burst in Texas, affecting water infrastructure due to power outages(Tiedmann, *et. al.*, 2023). These instances illustrate that climate change is undermining the stability of critical infrastructure across various countries and regions. Strengthening the resilience of critical infrastructure to climate change is crucial for sustainable social and economic development(Sathurshan, *et. al.*, 2022).

Infrastructure resilience is an evolving concept that refers to the ability to adapt to climate change and predict, withstand, or absorb various disaster risks(Cantelmi, *et. al.*, 2021). It is worth noting that despite the recognition of the necessity to operate and maintain systems like transportation, energy, and finance, these systems still exhibit significant vulnerabilities to extreme weather events(Wells, *et. al.*, 2022). Critical infrastructure, such as energy and transportation, often has complex interdependencies, where failure can have severe cascading effects on the overall system(Ongkowijoyo, *et. al.*, 2020). In addition, traditional infrastructure management relies heavily on visual inspections, manual measurements, and expert judgment, often involving single-field processes that are dependent on the manager's experience(Sánchez-Silva & Calderón-Guevara, 2022). Extreme weather like high temperatures and heavy rain increases the risk to managers working in such environments, affecting the continuity of the entire task process(Schulte, *et. al.*, 2023). Thus, traditional infrastructure management processes are fragmented, subjective, and ill-suited for managing interconnected complex systems.

Recent research trends indicate that integrating digital technology into critical infrastructure systems can enhance resilience to climate change through collaboration and support among various stakeholders(Shakou, *et. al.*, 2019). With the formalization of the Industry 4.0 wave, emerging technologies such as the Internet of Things (IoT), digital twins, artificial intelligence (AI), and Building Information Modeling (BIM) are revolutionizing infrastructure operations and management(Javaid, *et. al.*, 2022). The capabilities of digital tools for real-time data collection, processing, and analysis allow for rapid and accurate disaster risk prediction, assessment, and response, thereby helping to build climate adaptation capabilities in infrastructure systems. For instance, computer modeling can help predict and manage the impacts of wildfires and tropical cyclones on energy infrastructure intensified by rising temperatures(Teng, *et. al.*, 2021). However, the use of these technologies still faces significant challenges, including complex interdependencies, public privacy, and cybersecurity concerns(Merabti, *et. al.*, 2011). Additionally, the complexity of technology integration and high initial investment costs are significant obstacles that need to be addressed(McHenry, 2013).

As climate change accelerates, the urgency for governments and organizations to implement strategic plans to enhance the resilience of critical infrastructure is growing. This study aims to analyze the main opportunities and threats to integrating digital technology into infrastructure in the era of climate crisis. Through literature analysis, this paper first describes the scope and importance of critical infrastructure. It then identifies how digital technology can provide efficient and reliable decision making in an active or passive manner throughout the infrastructure lifecycle to enhance resilience. Finally, this study provides new technology-driven solutions for critical infrastructure asset management to address climate change challenges and promote sustainable development.

II. Literature Review

1. Critical Infrastructure

The term "critical infrastructure" is widely used in government and academic literature. It continues to evolve with changing societal needs because it represents a complex system. Nevertheless, researchers agree that critical infrastructure includes assets, systems, and networks vital to national security, public safety, and economic well-being, usually requiring special protection from relevant authorities(Gallais & Filiol, 2017). The United States has implemented extensive critical infrastructure protection programs since 1996, with the Department of Homeland Security's 2013 National Infrastructure Protection Plan (NIPP) identifying 16 critical infrastructures as vital pillars ensuring the nation's normal functioning(Savage, 2023). In the European Union, the European Program for Critical Infrastructure Protection (EPCIP) emphasizes to all member states and their citizens that an attack on or failure of Europe's critical infrastructure could have significant adverse impacts on neighboring countries(Lazari & Mikac, 2022). Table 1 shows the currently widely recognized critical infrastructure sectors and describes their components and functions.

Table 1. Classification and Description of Critical Infrastructure Sectors

Sector	Description
Energy Systems	It is divided into three interconnected parts: electricity, oil, and gas, and involves energy production, storage, and distribution.
Transportation Systems	Facilitates the movement of people and goods across different spaces, including aviation, road traffic, maritime and river transport, public transport, pipelines, and logistics.
Water Systems	This includes drinking water supply, wastewater treatment, and essential storage and control services.
Financial Systems	Includes banks, insurance companies, and critical financial utilities and services providers.
Healthcare and Public Health	Provides four key services to the public: hospital care, life-sustaining medical equipment supply, pharmaceuticals and blood supply, and diagnostic medical laboratories.

Food and Agriculture	Involves food supply, safety, and security.
Defense Industrial Base	Includes facilities for research, production, and maintenance of military resources and basic national security services.
Space	Provides communication support for ground infrastructure operations.
Chemical	Involves the use, production, storage, transportation, or delivery of chemicals and mixtures.
Information and Communication Technology	This involves identifying and mitigating cybersecurity threats and vulnerabilities, voice and data transmission, and data storage and processing.
Government Facilities	Includes various buildings within and outside the country that serve national functions, such as embassies, courts, and national laboratories.
Research Facilities	Applied for commercial or experimental research purposes.
Commercial Facilities	Places accommodating large crowds, such as hotels, commercial centers, office buildings, and stadiums.

Source: Alcaraz & Zeadally, 2015.

Critical infrastructure experiences increasing systemic failures that originate from minor disturbances but can ultimately lead to widespread impacts(Eusgeld & Dietz, 2011). In other words, the failure of one infrastructure can affect the functionality of other infrastructures. Numerous instances have proven that interconnections between critical infrastructure sectors have created significant interdependencies(Seppänen, *et. al.*, 2018). For example, in emergencies, rescue departments need fuel like diesel to power rescue vehicles and generators. However, urban flooding caused by heavy rainfall can damage roads, affecting the continuous supply from the energy sector and ultimately causing the entire system to fail.

The significant societal importance of these types of infrastructure and their interconnectivity means that adequate security measures must be identified to reduce the risk of failure(Duenas-Osorio & Vemuru, 2009). Therefore, considering these interdependencies is increasingly important when assessing the vulnerability of critical infrastructure. Their protection should be seen as a cross-sectoral activity, not confined to a specific sector(Kjølle, *et. al.*, 2012).

2. Climate Change and Critical Infrastructure Resilience

Traditionally, the management of critical infrastructure has focused on physical protection against threats to terrorism(Boin & Smith, 2006). However, with the increasing frequency and severity of extreme weather events such as floods, wildfires, hurricanes, and heatwaves due to global warming, the risks faced by critical infrastructure are also increasing(Leviäkangas & Michaelides, 2014). These extreme weather events can directly damage infrastructure and disrupt the supply chains that sustain their operation. Therefore, managing critical infrastructure has evolved into a broader approach, emphasizing resilience as a key attribute throughout its lifecycle(Guest, *et. al.*, 2020). In other words, managing critical infrastructure means managing its resilience.

Resilience is defined in various ways in the literature, mostly based on robustness and adaptability, aligning with pioneering ecological research(Opdyke, *et. al.*, 2017). Resilience is closely related to management and focuses on the ability to maintain performance levels when facing risks and the time and cost required to achieve these levels(Heinimann & Hatfield, 2017). Climate change disrupts the fundamental assumptions of traditional engineering systems that determine the critical performance of modern cities, necessitating innovative paradigms and new assumptions for designing more resilient critical infrastructure in the future(Bocchini, *et. al.*, 2014).

Furthermore, the increasing interconnections within and between critical infrastructure systems have made these systems interdependent and susceptible to cascading failures and institutional changes, leading to significant changes in system functionality(Rinaldi, *et. al.*, 2001). These changes include, but are not limited to, emergency disruptions of critical services, system damage, and even total system failure. Existing infrastructure standards often cannot adapt to the current climate; therefore, a lifecycle perspective is needed. Infrastructure resilience must be integrated into the planning, construction, operation, and maintenance phases(Liu, *et. al.*, 2019).

(1) Planning and Construction Phase

In the planning and construction phase, climate change requires re-evaluation of site selection, design, and material choices(Dong & Frangopol, 2020). Traditional site selection may overlook future flood risks, and design standards may not fully consider changes in extreme temperatures, storms, and rainfall(Izaddoost, *et. al.*, 2021). Therefore, introducing climate prediction data and risk assessment tools is necessary to develop more forward-looking design standards. For example, in flood-prone areas, higher levees and larger capacity drainage systems should be designed.

(2) Operation Phase

During the operational phase, extreme weather caused by climate change can disrupt the normal operation of the infrastructure. High temperatures may deform roads and tracks, storms may damage power and communication networks, and droughts may affect the supply and quality of water resources. Therefore, during operation, monitoring and emergency response mechanisms need to be strengthened(Wang, *et. al.*, 2021). For instance, power systems should be equipped with backup power sources and smart grid technology to ensure rapid power restoration during disasters.

(3) Maintenance Phase

In the maintenance phase, the frequent occurrence of extreme events due to climate change intensifies infrastructure aging and damage, increasing maintenance costs and difficulty(Capacci & Biondini, 2020). Regular assessments of infrastructure conditions, long-term maintenance plans, and adequate emergency supplies are required(Makhoul & Kromanis, 2023). For example, in windy areas, regular inspections and reinforcements of power poles and transmission towers are necessary to prevent large-scale power outages caused by storms.

As the challenges posed by climate change continue to grow, the management of critical infrastructure must shift to more resilient strategies, enhancing resilience in the planning, construction, operation, and maintenance phases through the introduction of advanced technologies and methods, ensuring stability and continuity during extreme weather events. Recent trends indicate that emerging digital technologies can address some of these issues(Argyroudis, *et. al.*, 2022). Digital and sensor technologies, data aggregation, and advanced simulation capabilities can automate these assessments. However, these technologies have not yet been fully utilized.

3. Digital Technology and Critical Infrastructure Asset Management

Critical infrastructure asset management is considered a multidisciplinary strategic and systematic comprehensive process for operating, maintaining, and improving physical assets(Too, 2010). Through strategic and systematic management of infrastructure assets, organizations can improve service delivery, extend asset life, reduce lifecycle costs, and minimize risks associated with asset failures(Kure & Islam, 2019). However, traditional infrastructure risk assessment and diagnosis rely mainly on inspections, supplemented by routine monitoring and analysis, making it challenging to provide comprehensive decision support(Parlikad & Jafari, 2016). In addition, risk-based management approaches struggle to handle "low probability, high consequence" events. For example, the 2011 Tohoku earthquake and the Fukushima Daiichi nuclear disaster did not account for infrastructure exceeding its design life, as existing risk models and assessment methods usually fail to explain such events(Cai & Golay, 2021). Moreover, neglecting the interdependencies between infrastructures can lead to inaccurate risk assessments of compound events.

In the era of smart infrastructure, widespread adoption of emerging digital technologies can address the problems and weaknesses of traditional management methods, fundamentally transforming infrastructure management. For instance, AI facilitates data mining and the integration of information and evidence, enabling near-real-time applications across different infrastructure systems(Sarker, 2024). These new technologies will pave the way for more accurate and automated decision making, thereby enhancing infrastructure safety. In addition, they provide end-users with the means to communicate, visualize, and interact with their ecosystem, thus strengthening their climate adaptation capabilities. For instance, real-time modeling based on 5G agents can improve substation accessibility for affected and interdependent infrastructure systems(Gan, *et. al.*, 2021).

Resilience analysis is a data-driven process that uses virtual modeling to make predictions(Sharma & Gardoni, 2018). This technology provides a method for visualizing critical infrastructure performance, identifying the impacts of interdependencies between different infrastructures to mitigate uncertainty, and ultimately facilitating decision-making prioritization. Emerging digital technologies and real-time data analysis enhance infrastructure climate adaptation capabilities more effectively than traditional methods. For example, IoT technology supports sustainable solutions to climate change by measuring carbon emission levels from traffic and building services to promote clean energy use(Hyman, *et. al.*, 2019). Another example is the deployment of resilience analysis to advance the quantification, evaluation, and comparison of management, making infrastructure assets more operational(Maletič, *et. al.*, 2020).

Emerging digital technologies offer more efficient, rapid, and reliable resilience assessments based on actionable performance indicators throughout the infrastructure lifecycle, enabling better decision-making. Table 2 shows recently emerged technologies and their impact on enhancing the climate adaptation capacity of critical infrastructure.

Table 2. Digital Technologies and Applications toward Climate Resilience of Infrastructure

Digital Technology	Definition	Climate Adaptation Performance
5G Technology (Shi, 2020)	Facilitates data mining and information integration between infrastructure systems by providing higher data transmission speeds, lower latency, and greater network capacity.	Real-time data transmission and monitoring enable rapid response to climate events, thereby reducing traffic problems caused by sudden weather changes.
Internet of Things (IoT) (Koo, *et. al.*, 2015)	Connects various physical devices through a network, providing data collection, communication, processing, and actionable intelligence for a range of applications, services, and decisions.	Real-time monitoring and data feedback help quickly address water supply issues caused by climate change, thus improving water resource management efficiency and safety.
Artificial Intelligence (AI) (Singh & Goyal, 2023)	Simulates human intelligence through computer systems, including machine learning, natural language processing, and image recognition technologies, especially computer systems that can learn and accumulate experience.	Predictive maintenance can reduce equipment damage and failures caused by climate change, thereby enhancing infrastructure reliability and continuity.
Building Information Modeling (BIM) (Ackerman, *et. al.*, 2019)	A three-dimensional digital model used to manage and exchange monitoring data to manage information related to the entire lifecycle of building assets.	Accurate simulation and optimized design improve building disaster resilience and energy efficiency, thereby reducing the impact of climate change on buildings.
Digital Twin (Kaewunruen, *et. al.*, 2022)	Digital replicas of physical assets, processes, and systems. Digital twins can monitor, analyze, and optimize the	Real-time monitoring and predictive analysis enhance the infrastructure response capability and optimization level, effectively

	performance of physical assets in real time.	addressing the challenges posed by climate change.

III. Opportunities and Challenges: Enhancing Critical Infrastructure Resilience through Digital Technologies

In addressing natural disasters related to climate change, digital technology offers many opportunities to significantly improve the efficiency, effectiveness, and reliability of critical infrastructure. The following are the specific applications of digital technology in this area:

(1) Real-time Monitoring and Rapid Response

Advanced digital technologies applied in critical infrastructure such as water networks, power grids, and transportation systems allow managers to continuously monitor structural integrity, temperature, and environmental conditions through sensors and IoT devices. For example, digital twins can monitor water pipelines, power lines, and transportation networks in real time, helping management continuously adjust operational conditions, quickly respond to service interruptions, and reduce potential risks. In addition, the availability of real-time data allows swift responses to anomalies or emergencies, enhancing system resilience and emergency capabilities(Storesund, *et. al.*, 2018).

(2) Predictive Maintenance

Predictive maintenance adopts a proactive asset management approach, which is particularly important in industries heavily reliant on equipment reliability, such as aviation and healthcare. AI is a core technology for predictive maintenance(Wang & Wang, 2018). For instance, machine learning models can predict when equipment or infrastructure components are likely to fail or need maintenance by analyzing historical data(Cardoso & Ferreira, 2020). This predictive maintenance method surpasses traditional response strategies by scheduling repairs and maintenance based on expected wear, thus preventing failures before they occur. Moreover, predictive maintenance can extend the service life of infrastructure and reduce the costs associated with emergency repairs(Achouch, *et. al.*, 2022).

(3) Enhanced Decision-making

Infrastructure asset management can be seen as a data-driven decision-making process. For example, BIM, which is widely used in the construction industry, can meet the needs of smart buildings by integrating with other information management systems(Yang & Peng, 2001). BIM technology can identify interdependencies between different infrastructures, mitigate uncertainty, and facilitate prioritization in final decision making. BIM also applies visualization functions to pipeline collision tests, energy consumption assessments, and emergency management, providing reliable bases for decision making throughout its lifecycle(Akbarieh, *et. al.*, 2020).

Despite the significant opportunities that digital technology offers for enhancing infrastructure resilience, its application also faces notable challenges:

(1) Cybersecurity Risks

As critical infrastructure becomes interconnected and reliant on digital technology, the cyber threats they face also increase(Roshanaei, 2021). Control systems are widely used in many critical infrastructures, including transportation, power plants, and nuclear power stations, typically computer-based facilities. In modern society, critical infrastructure is transitioning from isolated environments to public environments, requiring connection to public networks, thus becoming prime targets for cyberterrorism(Wilson, 2014). In addition, implementing digital technology in critical infrastructure management involves substantial data collection, storage, and analysis, which raises issues of personal privacy, data security, and potential misuse or leakage of information(Simola, 2020). Therefore, overreliance on digital systems may introduce new vulnerabilities, increasing cybersecurity risks.

(2) Human-machine Interaction Conflicts

In modern society, digital technology is increasingly integrated into the workplace. With the widespread transition to Industry 4.0, the use of collaborative robots in industrial environments has become indispensable(Hentout, *et. al.*, 2019). For example, in the chemical industry, operators can use inspection robots in confined hazardous spaces to check pipeline defects(Martinetti, *et. al.*, 2021). However, interacting with intelligent machines may increase operators' cognitive load because the process may involve complex operational steps. In addition, many frontline workers perceive collaborative robots as intended to replace them rather than alleviate their workload(Paul, *et. al.*, 2022). Therefore, human-machine interaction conflicts pose additional challenges and warnings for improving infrastructure digitization.

(3) Funding Barriers

Approximately 70% of greenhouse gas emissions come from critical infrastructures like power generation and industry. Although smart energy management systems can optimize energy consumption across different industries, reduce greenhouse gas emissions, and improve energy efficiency, integrating digital technology into existing infrastructure systems typically requires significant upfront investment(Osei-Kyei, *et. al.*, 2021). These costs usually include the purchase of technology, software, and equipment and the modification of existing systems to accommodate new technology. Additionally, stakeholders' reluctance to invest makes proactively building infrastructure resilience more challenging. For critical infrastructure, particularly in economically constrained regions, securing funding can be a major obstacle.

Strategically and systematically managing infrastructure assets and widely adopting emerging digital technologies can address the problems and weaknesses of traditional management methods, significantly enhancing infrastructure climate adaptation capabilities. However, overcoming the aforementioned challenges is crucial during implementation to ensure the effective application of digital technology and the long-term sustainable development of infrastructure.

IV. Conclusion

Emerging technologies pave the way for more accurate and automated decision making to achieve safer infrastructure while providing end-users with the means to communicate, visualize, and interact with the ecosystem. This study proposes some improvement measures and suggestions by analyzing the challenges posed by climate change to critical infrastructure and methods to enhance its resilience using digital technology. In the planning and construction phase, the introduction of climate prediction data and risk assessment tools is necessary to develop more forward-looking design standards. For example, in flood-prone areas, higher levees and larger capacity drainage systems should be designed to cope with potential future extreme weather events. Simultaneously, applying IoT and digital twin technology for real-time monitoring of critical infrastructure such as water supply, electricity, and transportation can timely detect and address anomalies. For instance, power systems should be equipped with backup power sources and smart grid technology to ensure rapid power restoration during disasters and minimize downtime. In addition, predictive maintenance using AI and machine learning can identify potential failures and perform preventive repairs in advance, extending the life of the infrastructure and reducing maintenance costs.

With the application of digital technology, cybersecurity risks for critical infrastructure increase, necessitating enhanced cybersecurity measures to ensure data security and privacy protection. Establish robust data encryption and access control mechanisms to prevent cyber-attacks and data breaches. In the digitization process, addressing human-machine interaction conflicts is essential to ensure technology effectively assists staff rather than burdening them. User-friendly interface design and operational training can reduce operators' cognitive load and improve efficiency. Moreover, exploring various funding channels, including government grants, private sector investment, and international aid, is necessary to address the high upfront investment required for digital technology integration. For instance, public-private partnership (PPP) models can attract private capital participation in infrastructure construction and maintenance by sharing the financial burden.

In summary, climate change poses severe challenges to critical infrastructure; however, the strategic and systematic introduction and application of digital technology can significantly enhance infrastructure resilience. Despite challenges such as cybersecurity and funding constraints, effective planning and management can achieve sustainable infrastructure development, ensuring stability and reliability during future extreme weather events.

References

Achouch, M., Dimitrova, M., Ziane, K., Sattarpanah Karganroudi, S., Dhouib, R., Ibrahim, H., & Adda, M. (2022). On predictive maintenance in industry 4.0: Overview, models, and challenges. *Applied Sciences*, 12(16), 8081.

Ackerman, A., Cave, J., Lin, C. Y., & Stillwell, K. (2019). Computational modeling for climate change: Simulating and visualizing a resilient landscape architecture design approach. *International Journal of Architectural Computing*, 17(2), 125-147.

Ahmed, I., & Ledger, K. (2023). Lessons from the 2019/2020 'Black Summer Bushfires' in Australia. *International journal of disaster risk reduction*, 96, 103947.

Akbarieh, A., Jayasinghe, L. B., Waldmann, D., & Teferle, F. N. (2020). BIM-based end-of-lifecycle decision making and digital deconstruction: Literature review. *Sustainability*, 12(7), 2670.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8, 53-66.

Argyroudis, S. A., Mitoulis, S. A., Chatzi, E., Baker, J. W., Brilakis, I., Gkoumas, K., ... & Linkov, I. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management*, 35, 100387.

Bocchini, P., Frangopol, D. M., Ummenhofer, T., & Zinke, T. (2014). Resilience and sustainability of civil infrastructure: Toward a unified approach. *Journal of Infrastructure Systems*, 20(2), 04014004.

Boin, A., & Smith, D. (2006). Terrorism and critical infrastructures: Implications for public–private crisis management. *Public Money and Management*, 26(5), 295-304.

Cai, Y., & Golay, M. W. (2021). A framework analyzing system status and human activities: Illustrated using 2011 Fukushima nuclear power plant accident scenarios. *Nuclear Engineering and Design*, 373, 111025.

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, 41(3), 341-376.

Capacci, L., & Biondini, F. (2020). Probabilistic life-cycle seismic resilience assessment of aging bridge networks considering infrastructure upgrading. *Structure and Infrastructure Engineering*, 16(4), 659-675.

Cardoso, D., & Ferreira, L. (2020). Application of predictive maintenance concepts using artificial intelligence tools. *Applied Sciences*, 11(1), 18.

Dong, Y., & Frangopol, D. M. (2020). Resilience of Civil Infrastructure in a Life-Cycle Context. *In Resilience of Critical Infrastructure Systems* (pp. 43-48). CRC Press.

Duenas-Osorio, L., & Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. *Structural safety*, 31(2), 157-167.

Eusgeld, I., Nan, C., & Dietz, S. (2011). "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6), 679-686.

Gallais, C., & Filiol, E. (2017). Critical infrastructure: Where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure. *Journal of Information Warfare*, 16(1), 64-87.

Gan, X., Geng, X., Xiong, Z., Wu, Z., Du, S., Gao, Y., & Guo, Y. (2021, July). Application of 5G communication technology on intelligent inspection in 750kV substation. *In Journal of Physics: Conference Series* (Vol. 1983, No. 1, p. 012089). IOP Publishing.

Guest, G., Zhang, J., Maadani, O., & Shirkhani, H. (2020). Incorporating the impacts of climate change into infrastructure life cycle assessments: A case study of pavement service life performance. *Journal of Industrial Ecology*, 24(2), 356-368.

Heinimann, H. R., & Hatfield, K. (2017). Infrastructure resilience assessment, management and governance–state and perspectives. *In Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains* (pp. 147-187). Springer Netherlands.

Hentout, A., Aouache, M., Maoudj, A., & Akli, I. (2019). Human–robot interaction in industrial collaborative robotics:

a literature review of the decade 2008–2017. *Advanced Robotics*, 33(15-16), 764-799.

Huddleston, P., Smith, T., White, I., & Elrick-Barr, C. (2022). Adapting critical infrastructure to climate change: A scoping review. *Environmental Science & Policy*, 135, 67-76.

Hyman, B. T., Alisha, Z., & Gordon, S. (2019). Secure controls for smart cities; applications in intelligent transportation systems and smart buildings. *International Journal of Science and Engineering Applications*, 8(6), 167-171.

Izaddoost, A., Naderpajouh, N., & Heravi, G. (2021). Integrating resilience into asset management of infrastructure systems with a focus on building facilities. *Journal of Building Engineering*, 44, 103304.

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Gonzalez, E. S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. *Sustainable Operations and Computers*, 3, 203-217.

Kaewunruen, S., AbdelHadi, M., Kongpuang, M., Pansuk, W., & Remennikov, A. M. (2022). Digital twins for managing railway bridge maintenance, resilience, and climate change adaptation. *Sensors*, 23(1), 252.

King-Okumu, C., Tsegai, D., Pandey, R. P., & Rees, G. (2020). Less to lose? Drought impact and vulnerability assessment in disadvantaged regions. *Water*, 12(4), 1136.

Kjølle, G. H., Utne, I. B., & Gjerde, O. (2012). Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety*, 105, 80-89.

Koo, D., Piratla, K., & Matthews, C. J. (2015). Towards sustainable water supply: schematic development of big data collection using internet of things (IoT). *Procedia engineering*, 118, 489-497.

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber□Physical Systems: Theory & Applications*, 4(4), 332-340.

Lazari, A., & Mikac, R. (2022). The External Dimension of European Union's Critical Infrastructure Protection Programme: From Neighboring Policy to Transatlantic Cooperation. *In The External Dimension of the European Union's Critical Infrastructure Protection Programme* (pp. 13-27). CRC Press.

Leviäkangas, P., & Michaelides, S. (2014). Transport system management under extreme weather risks: views to project appraisal, asset value protection and risk-aware system management. *Natural hazards*, 72(1), 263-286.

Liu, H. J., Love, P. E., Sing, M. C., Niu, B., & Zhao, J. (2019). Conceptual framework of life-cycle performance measurement: Ensuring the resilience of transport infrastructure assets. Transportation Research Part D: Transport and Environment, 77, 615-626.

Makhoul, N., & Kromanis, R. (2023). Toward enhancing community resilience: Life-cycle resilience of structural health monitoring systems. *In Life-Cycle of Structures and Infrastructure Systems* (pp. 295-302). CRC Press.

Maletič, D., Maletič, M., Al-Najjar, B., & Gomišček, B. (2020). An analysis of physical asset management core practices and their influence on operational performance. *Sustainability*, 12(21), 9097.

Martinetti, A., Chemweno, P. K., Nizamis, K., & Fosch-Villaronga, E. (2021). Redefining safety in light of human-robot interaction: A critical review of current standards and regulations. *Frontiers in chemical engineering*, 3, 666237.

McHenry, M. P. (2013). Technical and governance considerations for advanced metering infrastructure/smart meters: Technology, security, uncertainty, costs, benefits, and risks. *Energy Policy*, 59, 834-842.

Merabti, M., Kennedy, M., & Hurst, W. (2011, March). Critical infrastructure protection: A 21 st century challenge. *In 2011 International Conference on Communications and Information Technology (ICCIT)* (pp. 1-6). IEEE.

Ongkowijoyo, C. S., Doloi, H., & Gurmu, A. T. (2020). Hybrid risk analysis model for analyzing the urban infrastructure risk. *International Journal of Disaster Risk Reduction*, 48, 101600.

Opdyke, A., Javernick-Will, A., & Koschmann, M. (2017). Infrastructure hazard resilience trends: an analysis of 25 years of research. *Natural hazards*, 87(2), 773-789.

Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction*, 60, 102316.

Parlikad, A. K., & Jafari, M. (2016). Challenges in infrastructure asset management. *IFAC-PapersOnLine*, 49(28), 185-190.

Paul, S., Yuan, L., Jain, H. K., Robert Jr, L. P., Spohrer, J., & Lifshitz-Assaf, H. (2022). Intelligence augmentation: Human factors in AI and future of work. *AIS Transactions on Human-Computer Interaction*, 14(3), 426-445.

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.

Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. *Journal of Computer and Communications*, 9(8), 80-102.

Sánchez-Silva, M., & Calderón-Guevara, W. (2022). Flexibility and adaptability within the context of decision-making in infrastructure management. *Structure and Infrastructure Engineering*, 18(7), 950-966.

Sarker, I. H. (2024). AI for Critical Infrastructure Protection and Resilience. *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*, 153-172.

Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: a systematic literature review of measurement frameworks. *Infrastructures*, 7(5), 67.

Savage, M. D. (2023). Critical Infrastructure and Key Resources. *In The Handbook of Homeland Security* (pp. 25-29). CRC Press.

Schulte, P. A., Jacklitsch, B. L., Bhattacharya, A., Chun, H., Edwards, N., Elliott, K. C., ... & Vietas, J. (2023). Updated assessment of occupational safety and health hazards of climate change. *Journal of occupational and environmental hygiene*, 20(5-6), 183-206.

Seppänen, H., Luokkala, P., Zhang, Z., Torkki, P., & Virrantaus, K. (2018). Critical infrastructure vulnerability—A method for identifying the infrastructure service failure interdependencies. *International Journal of Critical Infrastructure Protection*, 22, 25-38.

Shakou, L. M., Wybo, J. L., Reniers, G., & Boustras, G. (2019). Developing an innovative framework for enhancing the resilience of critical infrastructure to climate change. *Safety science*, 118, 364-378.

Sharma, N., Tabandeh, A., & Gardoni, P. (2018). Resilience analysis: A mathematical formulation to model resilience of engineering systems. *Sustainable and Resilient Infrastructure*, 3(2), 49-67.

Shi, X. (2020). More than smart pavements: connected infrastructure paves the way for enhanced winter safety and mobility on highways. *Journal of Infrastructure Preservation and Resilience*, 1(1), 13.

Simola, J. (2020). Privacy issues and critical infrastructure protection. *In Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 197-226). Academic Press.

Singh, S., & Goyal, M. K. (2023). Enhancing climate resilience in businesses: the role of artificial intelligence. *Journal of Cleaner Production*, 418, 138228.

Storesund, K., Reitan, N. K., Sjöström, J., Rød, B., Guay, F., Almeida, R., & Theocharidou, M. (2018). Novel methodologies for analysing critical infrastructure resilience. *In Safety and reliability–safe societies in a changing world* (pp. 1221-1229). CRC Press.

Suzuki, T., Tajima, Y., Watanabe, M., Tsuruta, N., Takagi, H., Takabatake, T., ... & Arikawa, T. (2020). Post-event survey of locally concentrated disaster due to 2019 Typhoon Faxai along the western shore of Tokyo Bay, Japan. *Coastal Engineering Journal*, 62(2), 146-158.

Teng, S. Y., Touš, M., Leong, W. D., How, B. S., Lam, H. L., & Máša, V. (2021). Recent advances on industrial data-driven energy savings: Digital twins and infrastructures. *Renewable and Sustainable Energy Reviews*, 135, 110208.

Tiedmann, H. R., Spearing, L. A., Castellanos, S., Stephens, K. K., Sela, L., & Faust, K. M. (2023). Tracking the post-disaster evolution of water infrastructure resilience: A study of the 2021 Texas winter storm. *Sustainable Cities and Society*, 91, 104417.

Too, E. G. (2010). A framework for strategic infrastructure asset management. *Definitions, concepts and scope of engineering asset management*, 31-62.

Wang, K., & Wang, Y. (2018). How AI affects the future predictive maintenance: a primer of deep learning. *In Advanced Manufacturing and Automation VII 7* (pp. 1-9). Springer Singapore.

Wang, M., Zhang, Y., Zhang, D., Zheng, Y., Li, S., & Tan, S. K. (2021). Life-cycle cost analysis and resilience consideration for coupled grey infrastructure and low-impact development practices. *Sustainable Cities and Society*, 75, 103358.

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in disaster science*, 15, 100244.

Wilson, C. (2014). Cyber threats to critical information infrastructure. *In Cyberterrorism: Understanding, Assessment, and Response* (pp. 123-136). New York, NY: Springer New York.

Yang, J., & Peng, H. (2001). Decision support to the application of intelligent building technologies. *Renewable energy*, 22(1-3), 67-77.