Distributed Resilience Assessment of Critical Infrastructures with Digital Twins Considering Uncertainty

Tobias Gebhard
Institute for the Protection of Terrestrial Infrastructures
German Aerospace Center (DLR)
Darmstadt, Germany
tobias.gebhard@dlr.de

Andrea Tundis
Institute for the Protection of Terrestrial Infrastructures
German Aerospace Center (DLR)
Darmstadt, Germany
andrea.tundis@dlr.de

***Abstract*—The increasing complexity and interconnectivity of critical infrastructures such as power systems - driven for example by the integration of Internet of Things (IoT) technologies - require understanding and evaluation of their resilience to cyber-physical threats. Digital Twins are a promising tool for analyzing system behavior under stress, e.g. failures and overloads, in a controlled environment. This paper presents a probabilistic simulation-based resilience assessment framework as a Digital Twin approach. Focusing on power systems, we consider cyber-physical threat scenarios, including IoT-based load altering attacks, where compromised smart devices manipulate demand patterns to destabilize the grid. By considering the inherent uncertainty of crises in impact modeling, a distributed computing approach enables simulating a diverse, randomized set of scenarios with high sampling size, allowing for a comprehensive estimation of resilience properties. Results demonstrate how different impact intensities and system configurations affect system performance, characterized by different resilience metrics. Our holistic approach improves risk and resilience analysis of critical infrastructures by incorporating uncertainty into quantitative assessments, supporting crisis management and decision-making.**

***Index Terms*—Critical Infrastructures, Resilience Assessment, Digital Twin, Load Altering Attack, Monte-Carlo-Simulation**

I. Introduction

Critical infrastructures (CIs) are increasingly becoming interconnected, for example due to the integration of Internet of Things (IoT) technologies into power systems. While this digitalization enables real-time data exchange, improved operational efficiency, and leverages transformative tools like Digital Twins (DTs), it also introduces new cyber-physical threats [1]. The interdependencies between systems—such as energy, water, and transportation—can lead to cascading failures [2] and, in worst-case scenarios, large-scale blackouts, highlighted for example by the massive power outage in Ukraine in 2015 [3]. The exposure of CIs to such high-impact, low-probability (HILP) events, whether caused by man-made threats (e.g., cyber attacks, terrorist attacks) or natural hazards (e.g., floods, tornadoes, earthquakes) underline the need for comprehensive resilience assessments [4].

The increasing connectivity of smart devices also introduces new risks specific to power grids. IoT-based hacking attacks, such as load altering attacks, can force compromised devices to simultaneously surge power demand, endangering grid stability [5]. Moreover, social engineering attacks on demand response systems further exacerbate this problem by triggering unwanted load synchronization [6], [7]. Due to the inherently low load factor of power demand, such synchronized spikes can impose significantly higher stress than average operational levels, potentially leading to blackouts or grid instability [8]. Consequently, analyzing and understanding the vulnerability and resilience of power systems to HILP events is essential for minimizing disruptions and protecting public safety [9].

Simulation-based models provide a powerful means to analyze cyber-physical systems (CPS), as they allow testing of severe disruption scenarios under various conditions that would be impractical or too dangerous to conduct on real-world infrastructure [10]. Digital Twins, real-time virtual representations of physical systems, offer a promising tool for this task by providing simulation capabilities with sufficient computing resources, enabling comprehensive assessments of system resilience [11]. Resilience, defined as the ability of a system to withstand and recover from disruptive events while maintaining a certain level of functional operation, is a key concept in disaster risk management [12]. Quantitative resilience assessment is crucial for comparing cost-intensive CI hardening alternatives and guiding policy makers for strategic investments in resilience on a grounded basis [4].

However, the inherent uncertainty in natural disasters and cyber-physical threats makes disaster planning and resilience assessment challenging. Hazard scenarios may differ in frequency, intensity, geographic scale, and environmental conditions, e.g. extreme weather [4], [13]. Moreover, differences in human behavior may result in significantly varying outcomes [14]. For these reasons, a holistic resilience analysis requires a

The research activities related to this work have been conducted in the context of the "urbanModel" project funded from the German Aerospace Center (DLR). This work has been performed in the context of the LOEWE center emergenCITY [LOEWE/1/12/519/03/05.001(0016)/72].

2325-2944/25/$31.00 ©2025 IEEE
DOI 10.1109/DCOSS-IoT65416.2025.00150

probabilistic approach to address this uncertainty, using several scenario simulations to capture a wide range of possible outcomes.

In this paper, we introduce a probabilistic simulation-based resilience assessment framework for CIs. We propose a quantitative, performance-based approach, incorporating Monte-Carlo-Simulation (MCS) for random sampling, to systematically capture uncertainty and evaluate the impact of varying impact intensities and system conditions. Resilience metrics are computed for each simulation run and collected for statistical analysis. Due to the possibility of parallelizing individual simulations, the approach can be applied with distributed computation, e.g. using cloud computing, enabling high sampling sizes and scalability.

In a case study, we focus on the power system as the most fundamental CI and apply our methodology using cyber attack scenarios on IoT devices and grid components, leading to overloads or component failures. We analyze the resilience of an urban medium-voltage power grid and compare resilience metrics for two system configurations, providing insights in the implications of different control strategies. A graph-based, quasi-dynamic power grid model is used, including cascading outage simulations. Moreover, a probabilistic sensitivity analysis is performed to characterize system robustness under varying attack intensity.

Our findings highlight the importance of incorporating uncertainty into resilience and risk management practices. By quantifying resilience under diverse threat scenarios, our approach supports CI vulnerability analysis and quantitative resilience assessment against HILP events. This proactive approach can inform targeted investments in grid hardening to mitigate the impact of disruptive events and cascading failures, ultimately contributing to maintaining uninterrupted service of CIs.

The remainder of this paper is structured as follows: Section II provides an overview of Digital Twins for CIs and discusses their role in resilience assessment. Section III details our stochastic resilience assessment methodology. Section IV presents the case study and results, while Section V concludes and provides implications for future research and practical applications.

II. Background on Digital Twins for Critical Infrastructures

Digital Twins (DTs) are virtual representations of physical systems that integrate real-time data, simulation models, and analytics to enable comprehensive what-if analysis, optimization, and decision-making [15], [16]. They have emerged as a transformative technology, particularly in the IoT Edge-Cloud Continuum, allowing for advanced monitoring and prediction [17]. Over recent years, research on DTs has expanded across various disciplines, e.g. manufacturing, building information modeling (BIM), transportation, and energy. DT is considered a promising key technology for several power system applications [18].

Traditionally, DTs have been widely implemented in industrial settings, leveraging big data and artificial intelligence (AI) for optimization and automation [15]. However, their application in disaster risk management has recently gained traction [19]–[21]. Unlike industrial environments where massive data facilitate AI-driven approaches [22], CI systems often face data scarcity, particularly regarding HILP events [11]. Therefore, physical modeling and simulation-based bottom-up approaches are essential to analyze emergent and cascading effects in CIs [11]. DTs can provide a controlled sandbox environment for the creation of virtual clones and analysis of what-if scenarios [20]. Through such simulations, cascading effects across multiple CI sectors, including power, water, and transportation, can be analyzed to gain a more holistic perspective [11].

Given their simulation capabilities, DTs provide a powerful framework for resilience assessment by simulating and evaluating the impacts of various potential disruptive events on CI systems [11]. They can enable the study of system behavior under different stress scenarios, allowing for the comparative assessment of, e.g., different system configurations, control strategies, or alternative infrastructure hardening optimizations. By integrating social modeling, urban DTs can also be used to predict demand and mobility patterns, demonstrating their potential to improve the resilience of cities [11], [14], [23].

In addition to offline scenario analysis, DTs can also offer real-time resilience monitoring [11]. By integrating real-time data streams from sensor networks and simulation outputs, DTs can provide early warning mechanisms and proactive risk management capabilities. This dynamic monitoring can support decision-makers in responding swiftly to emerging threats, ultimately contributing to more resilient and adaptive infrastructure systems.

III. Stochastic Resilience Assessment Methodology

This section presents our proposed methodology for stochastic resilience assessment. An overview of the approach is depicted in Figure 1.

A. Resilience Assessment for Critical Infrastructures

Assessing resilience is essential for grounded evaluation of CI performance under different conditions, allowing effective comparability. While the assessment can be qualitative and/or empirical, we focus on performance-based resilience assessment through sandbox simulations. Considering a wide spectrum of possible scenarios without being restricted to historic events is crucial for a holistic view to capture the full range of possible outcomes [11]. While specified resilience can be assessed for a specific hazard type, general resilience requires a broader consideration of diverse threat scenarios [11]. These threats may include floods, hurricanes, pandemics, or earthquakes, all of which can impact the resilience of CIs [24].

B. Resilience Metrics

Quantitative resilience assessment involves the definition of resilience metrics, which can be categorized into performance

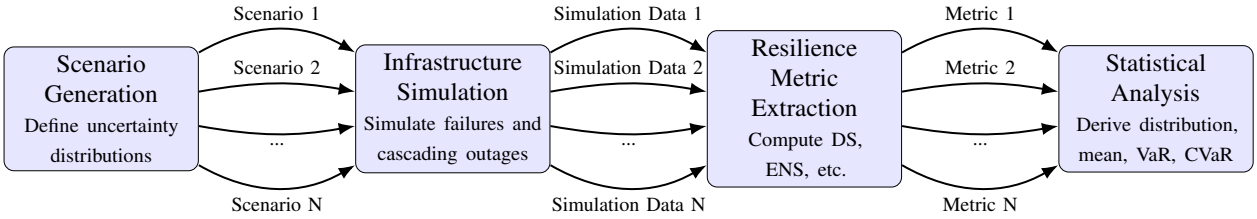

Fig. 1. Flow Diagram for the proposed distributed stochastic resilience assessment. Predefined scenarios with uncertain parameters are randomly generated using Monte-Carlo-Simulation (MCS). After performing a simulation for each scenario, a scalar resilience metric is calculated on the simulation data. The distribution of resulting values can be analyzed and formed into a single value, characterizing the resilience of the system.

metrics and summary metrics [25], [26]. Performance metrics measure system performance over time, while summary metrics provide a single value representation of resilience for a certain scenario [25].

In the context of power systems, the demand satisfaction (DS) is commonly used as a measure for system performance [10], [26] and defined as the normalized ratio of supply and demand:

$$DS(t) = \frac{\text{Supplied Load}(t)}{\text{Demand}(t)} \in [0, 1] \tag{1}$$

A similar metric is the *Load Not Supplied* (LNS):

$$LNS(t) = \text{Demand}(t) - \text{Supplied Load}(t) \tag{2}$$

A widely used summary metric is the *Energy Not Supplied* (ENS), calculated as the integral of LNS(t) over the event, and commonly used for risk management and reliability assessment [27]. In this study, we focus on the minimal DS or maximal LNS during the absorption phase as a robustness metric, representing absorptive capacity [10], [12].

C. Scenario Generation and Simulation using Distributed Computing

Since hazards cannot be seen as fixed scenarios, we consider a stochastic approach for resilience assessment. Any crisis scenario involves uncertainty, which can be represented as probability distributions. Also, internal or environmental conditions, such as power demand need to be seen as random variable [8].

To address this uncertainty, we consider Monte-Carlo-Simulation (MCS) for randomly sampling parameterized scenarios. This involves repeatedly simulating the base system under varying conditions, such as geographic impact area and event intensity, drawn from a given probability distribution. The CI model then simulates component outages and cascading effects depending on failures and overloads. Affected CI components (e.g. power buses or lines) are identified based on impact intensity parameters, their individual susceptibility to the type of event, and other factors, for example the geographic proximity to the impact location.

We propose the use of distributed computing to achieve a high number of samples efficiently. By leveraging cloud-based parallel computing, computation time can be significantly reduced, while maintaining high sampling numbers. Nevertheless, to handle the substantial computational resources for MCS, model complexity is an important consideration [11]. The principle of parsimony suggests that models should be as simple as possible while still capturing all relevant real-world features.

D. Resilience Distribution

Each simulation run produces a resilience metric, resulting in a distribution of values with a cumulative distribution function (CDF) F_R that can be analyzed statistically. A histogram of the resilience metric can provide insight into the statistical distribution of system behavior. The expected value $\mathrm{E}(R)$ of a resilience metric R ("expected resilience") represents the average system performance [28]. However, resilience optimization based solely on the mean value can be misleading, as it does not consider HILP events accordingly [13], [27].

To better account for HILP events, tail-oriented metrics such as Value at Risk (VaR) and Conditional Value at Risk (CVaR) can be used. CVaR quantifies the expected resilience loss in the worst-case scenarios, above the VaR $F_R^{-1}(1-\alpha)$, capturing the impact of HILP events as:

$$\mathrm{CVaR}_{1-\alpha}(R) = \mathrm{E}\left(R | R > F_R^{-1}(1-\alpha)\right) \tag{3}$$

By analyzing the tail of the resilience metric distribution, risk-averse strategies for infrastructure protection and crisis management can be developed.

IV. Case Study: Simulation-based Resilience Assessment of Urban Power Grid

In order to demonstrate the applicability of our proposed framework, we conduct a case study on an urban medium-voltage (MV) grid representing a medium-sized German city. The synthetic grid is reconstructed using the methodology described in [29], which yields realistic spatial and electrical characteristics. We consider disturbances induced by cyber attacks on IoT devices and grid components. We analyze the impact of overloads and random point failures and compare system performance among the scenarios and two system configurations using different resilience statistics.

A. Simulation Setup

The MV grid model comprises interconnected buses, substations, and loads, and is simulated using the AC power flow model. The model is implemented using the open-source Python

tool *pandapower* [30]. By repeatedly solving the power flow, we perform quasi-dynamic simulations to model cascading outages due failures or overloads. This model may not be able to capture detailed behavior like electromagnetic transient effects, but is usually suited to represent the general system characteristics.

Two grid configurations are considered for comparison:

- **Interconnected:** Tie switches between MV substations are closed, allowing for meshed operation.
- **Separated:** Tie switches remain open, enforcing a radial operation.

Although the network topology remains identical in both cases, the operational mode influences the grid's capability to absorb disturbances.

B. Threat Scenario Generation

To analyze potential impacts of the cyber-attacks, we consider two types of specific impact:

- **Scenario A: Overload** — In this scenario, nodes are forced to operate at a higher load level due to the manipulation of IoT-connected devices. The increase in load is represented by an overload factor, and a hack success probability is applied, as not all nodes might be affected.
- **Scenario B: Random k-Component Failure** — Here, the attack or an accidental failure results in the shutdown of a set of nodes. We simulate this by randomly deactivating k buses, following the N-k contingency framework.

For both scenarios, the loads are modeled as (independent) normally distributed variables with standard deviation being 0.2 of the mean to represent uncertain variations in power demand.

C. Failure Modeling

Overload-induced failures are modeled using protective tripping logic: whenever a line or transformer exceeds the threshold of 100% loading, a nearby switch is triggered, deactivating the affected line branch. This mechanism initiates cascading outages, which are captured by iteratively recalculating the power flow after deactivating failed components until a new static state is reached. Voltage stability or dynamic protection schemes are not explicitly modeled.

D. Results A: Overload Sensitivity Analysis

We perform a sensitivity analysis by increasing the overload factor and hack success probability continuously. The summary metric used for this resilience assessment is the minimum demand satisfaction (DS) (1) during the absorption phase as a measure for robustness.

In Figure 2, the minimum DS is plotted against varying overload factors, assuming all nodes in the system are affected, for both grid configurations. The results show a sharp transition, indicating a percolation effect, where the system suddenly shifts from a stable state to widespread failures. Notably, the separated configuration appears more robust, whereas the interconnected configuration exhibits more cascading failures due to the meshed grid topology.

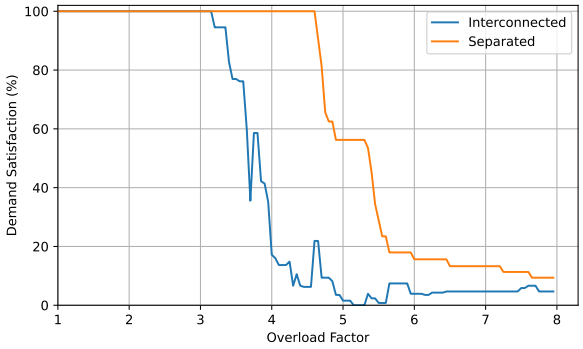

Fig. 2. Demand satisfaction (DS) for varying overload factors for both grid configurations.

In a complementary analysis (see Figure 3), DS is shown for a fixed overload factor of 7 and as a function of the attack probability that a node is affected. This result demonstrates a smoother transition but still confirms the relative advantage of the separated grid under coordinated load stress.

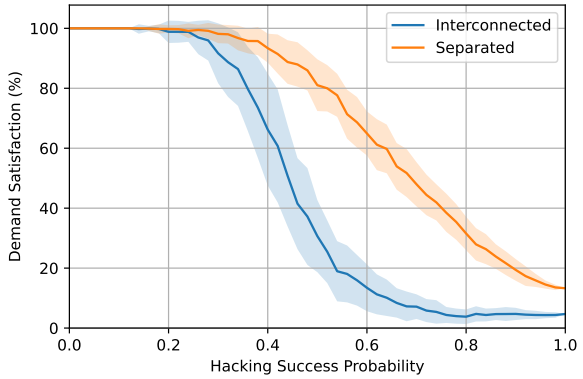

Fig. 3. Mean and standard deviation of DS for an overload factor of 7 as a function of the attack probability of a node being affected.

E. Results B: Random Point Failures

Now, we analyze the impact of k random bus failures. Here, the LNS metric (2), resulting from the outages, is used. The stochastic methodology is applied to generate a statistical distribution of the metric.

Figure 4 presents the histogram of LNS for $k = 5$ random bus failures. The histogram exhibits a fat-tailed distribution, with a mean of 1.68 MW and a maximum impact of 7.87 MW.

Additionally, Figures 5 and 6 display boxplots for different values of k, ranging from 0 to 20, for both configurations, respectively. Here, the interconnected grid achieves better robustness in average, especially for small k, as remaining buses can be supplied from the other side of an MV line, ensuring $N - 1$ security.

The results also reveal that while most random failures lead to limited impacts, rare extreme cases occur that represent the

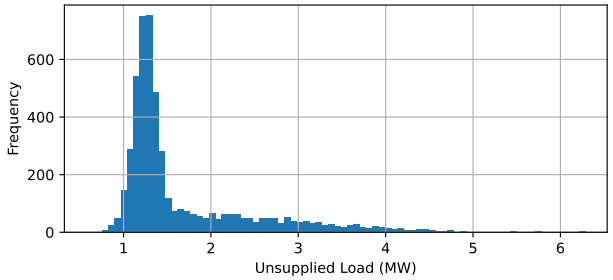

Fig. 4. Histogram of unsupplied load (LNS) for $k = 5$ bus outages in the interconnected configuration, showing a fat-tailed distribution.

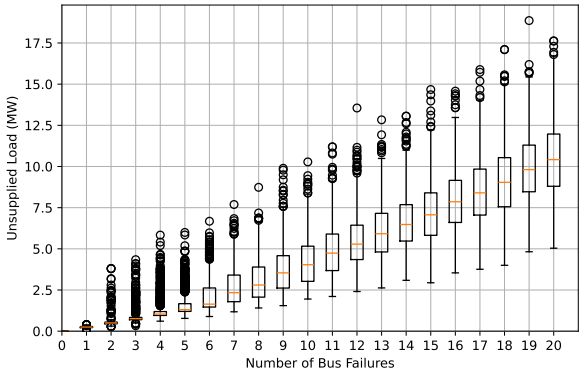

Fig. 5. Boxplot of unsupplied load for different k (interconnected). Boxes indicate the interquartile range (Q1–Q3).

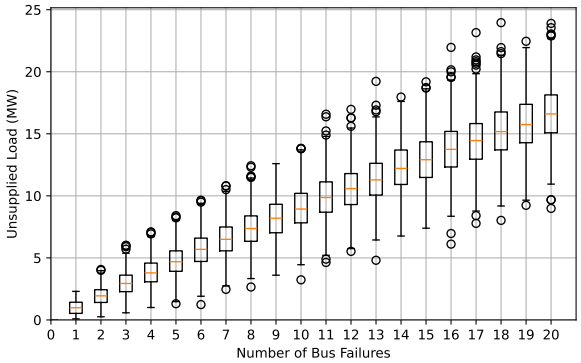

Fig. 6. Boxplot of unsupplied load for different k (separated). Boxes indicate the interquartile range (Q1–Q3).

tail of the distribution, which requires special attention. This also represents a vulnerability if the failures are no longer independent, as attackers could focus on these worst-case combinations.

F. Resilience Comparison

To directly compare the resilience of the two grid configurations, the metric distributions are condensed into summary statistics. Table I summarizes the mean, standard deviation, VaR (at $\alpha = 99\%$), CVaR, and the maximum value of the LNS metric for both random point failures ($k = 3$) and overload scenarios (factor 7, $p = 0.35$).

TABLE I
RESILIENCE METRIC DISTRIBUTION STATISTICS (LNS)

Statistic	Overload		Random Point	
	Interconnected	Separated	Interconnected	Separated
Mean	35.831	7.479	0.895	2.924
Std	29.420	8.965	0.489	0.932
VaR (99%)	121.250	33.000	3.228	5.162
CVaR (99%)	133.010	37.738	3.610	5.447
Max	159.250	53.500	4.246	6.196

The results reveal that for random point failures, the interconnected configuration exhibits less average interruption compared to the separated configuration, although the VaR and CVaR indicate that worst-case combinations can lead to losses of comparable impact. In contrast, for the overload scenario, the separated configuration demonstrates superior performance, with lower mean impact and reduced tail risk. This trade-off suggests that while the interconnected grid benefits from redundancy and rerouting capabilities under random failures, it is more susceptible to overloads and cascading effects.

V. Conclusion and Future Work

In this work, we presented a simulation-based resilience assessment framework for power systems within Digital Twins, incorporating uncertainty through MCS. We demonstrated how the proposed approach can be applied to gain insights into system resilience, considering IoT-based load altering attacks and random failures, and analyzed the influence of grid configurations. A sensitivity analysis on impact intensity and hacking success rate revealed emergent behavior, with percolation-like transitions and fat-tailed distributions in the resulting resilience metric. This suggests that even small changes in scenario parameters or system configurations can lead to dramatically different outcomes—information that is crucial for robust infrastructure planning.

Our findings highlight the importance of explicitly considering uncertainty in resilience assessments. The stochastic nature of critical impacts like HILP events on CIs underlines the necessity of a probabilistic approach rather than relying on deterministic, single-scenario evaluations. Our approach can serve as a basis for future resilience studies to provide grounded assessments, e.g. for comparing alternatives for CI optimization.

Looking forward, Digital Twins hold promise for real-time resilience monitoring and decision support during crises. Future work should explore the integration of more advanced software platforms for distributed computing utilizing cloud and edge computing resources to enable faster and scalable simulation-based assessments. Considering the possibility of using artificial neural networks (ANNs) for solving power flow [31] in combination with the continuous advances in hardware for generative AI, employing GPU architectures could be a viable approach for further parallelizing simulations,

enhancing computational efficiency and enabling quick large-scale assessments.

Furthermore, expanding the scope beyond power systems to include cascading effects in interdependent infrastructures (e.g., water, transport), incorporating geospatial hazard modeling, and simulating compound crises will offer a more holistic understanding of CI resilience.

REFERENCES

[1] T. Yang, Y. Liu, and W. Li, "Attack and defence methods in cyber-physical power system," *IET Energy Systems Integration*, vol. 4, no. 2, pp. 159–170, Apr. 2022.

[2] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[3] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[4] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power systems resilience assessment: Hardening and smart operational enhancement strategies," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1202–1213, Jul. 2017.

[5] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[6] G. Raman, B. AlShebli, M. Waniek, T. Rahwan, and J. C.-H. Peng, "How weaponizing disinformation can bring down a city's power grid," *PLOS ONE*, vol. 15, no. 8, p. e0236517, Dec. 2020.

[7] I. N. Grieser, T. Gebhard, A. Tundis, J. Kersten, T. Elßner, and F. Steinke, "Modeling and monitoring social media dynamics to predict electricity demand peaks," *Energy Reports*, vol. 13, pp. 1548–1557, Jun. 2025.

[8] T. Gebhard, E. Brucherseifer, and F. Steinke, "Monitoring electricity demand synchronization using copulas," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Oct. 2022.

[9] I. B. Sperstad, G. H. Kjølle, and O. Gjerde, "A comprehensive framework for vulnerability analysis of extraordinary events in power systems," *Reliability Engineering & System Safety*, vol. 196, p. 106788, Apr. 2020.

[10] B. Cassottana, M. M. Roomi, D. Mashima, and G. Sansavini, "Resilience analysis of cyber-physical systems: A review of models and methods," *Risk Analysis*, vol. 43, no. 11, pp. 2359–2379, 2023.

[11] T. Gebhard, B. J. Sattler, J. Gunkel, M. Marquard, and A. Tundis, "Improving the resilience of socio-technical urban critical infrastructures with digital twins: Challenges, concepts, and modeling," *Sustainability Analytics and Modeling*, vol. 5, p. 100036, 2024.

[12] A. Mentges, L. Halekotte, M. Schneider, T. Demmer, and D. Lichte, "A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures," *International Journal of Disaster Risk Reduction*, p. 103893, Jul. 2023.

[13] W. Li, E. A. Martínez Ceseña, L. S. Cunningham, M. Panteli, D. M. Schultz, S. Mander, C. Kim Gan, and P. Mancarella, "Assessing power system resilience to floods: A geo-referenced statistical model for substation inundation failures," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Oct. 2022, pp. 1–5.

[14] B. J. Sattler, A. Tundis, J. Friesen, and P. F. Pelz, "Modeling water availability during a blackout under consideration of uncertain demand response," in *The 3rd International Joint Conference on Water Distribution Systems Analysis & Computing and Control for the Water Industry (WDSA/CCWI 2024)*. MDPI, Sep. 2024, p. 130.

[15] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108 952–108 971, 2020.

[16] G. Fortino and C. Savaglio, "Integration of digital twins & internet of things," N. Crespi, A. T. Drobot, and R. Minerva, Eds. Cham: Springer International Publishing, 2023, pp. 205–225. [Online]. Available: https://doi.org/10.1007/978-3-031-21343-4_8

[17] C. Savaglio, V. Barbuto, F. Mangione, and G. Fortino, "Generative digital twins: A novel approach in the iot edge-cloud continuum," *IEEE Internet of Things Magazine*, vol. 8, no. 1, pp. 42–48, Jan. 2025.

[18] Z. Song, C. M. Hackl, A. Anand, A. Thommessen, J. Petzschmann, O. Kamel, R. Braunbehrens, A. Kaifel, C. Roos, and S. Hauptmann, "Digital twins for the future power system: An overview and a future perspective," *Sustainability*, vol. 15, no. 6, p. 5259, Jan. 2023.

[19] C. Fan, C. Zhang, A. Yahja, and A. Mostafavi, "Disaster city digital twin: A vision for integrating artificial and human intelligence for disaster management," *International Journal of Information Management*, vol. 56, p. 102049, Feb. 2021.

[20] E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, and M. Hellmann, "Digital twin conceptual framework for improving critical infrastructure resilience," *at - Automatisierungstechnik*, vol. 69, no. 12, pp. 1062–1080, Nov. 2021.

[21] M. R. M. F. Ariyachandra and G. Wedawatta, "Digital twin smart cities for disaster risk management: A review of evolving concepts," *Sustainability*, vol. 15, no. 15, p. 11910, Jan. 2023.

[22] M. M. Rathore, S. A. Shah, D. Shukla, E. Bentafat, and S. Bakiras, "The role of ai, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities," *IEEE Access*, vol. 9, pp. 32 030–32 052, 2021.

[23] J. Gunkel, M. Mühlhäuser, and A. Tundis, "Machine learning for human mobility during disasters: A systematic literature review," *Progress in Disaster Science*, vol. 25, p. 100405, Jan. 2025.

[24] E. M. Wells, M. Boden, I. Tseytlin, and I. Linkov, "Modeling critical infrastructure resilience under compounding threats: A systematic literature review," *Progress in Disaster Science*, vol. 15, p. 100244, Oct. 2022.

[25] C. Poulin and M. B. Kane, "Infrastructure resilience curves: Performance measures and summary metrics," *Reliability Engineering & System Safety*, vol. 216, p. 107926, Dec. 2021.

[26] H. Raoufi, V. Vahidinasab, and K. Mehran, "Power systems resilience metrics: A comprehensive review of challenges and outlook," *Sustainability*, vol. 12, no. 22, p. 9698, Nov. 2020.

[27] R. Moreno, M. Panteli, P. Mancarella, H. Rudnick, T. Lagos, A. Navarro, F. Ordonez, and J. C. Araneda, "From reliability to resilience: Planning the grid against the extremes," *IEEE Power and Energy Magazine*, vol. 18, no. 4, pp. 41–53, Jul. 2020.

[28] M. Ouyang and L. Dueñas-Osorio, "Multi-dimensional hurricane resilience assessment of electric power systems," *Structural Safety*, vol. 48, pp. 15–24, May 2014.

[29] T. Gebhard, A. Tundis, and F. Steinke, "Automated generation of urban medium-voltage grids using openstreetmap data," in *2024 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*. IEEE, Oct. 2024, pp. 1–5.

[30] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "Pandapower—an open-source python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6510–6521, Nov. 2018.

[31] R. Nellikkath and S. Chatzivasileiadis, "Physics-informed neural networks for ac optimal power flow," *Electric Power Systems Research*, vol. 212, p. 108412, Nov. 2022.