applied sciences

MDPI

Review

Measuring Resilience in Smart Infrastructures: A Comprehensive Review of Metrics and Methods

Abdulaziz Almaleh

Information Systems Department, King Khalid University, Abha 62529, Saudi Arabia; ajoyrulah@kku.edu.sa

Abstract: In today's world, the safety, economic prosperity, and social well-being of nations depend heavily on highly interconnected critical infrastructures. These infrastructures encompass power networks, natural gas systems, communication networks, water treatment facilities, and transportation systems. Gaining insight into the behavior of these infrastructures, particularly during stress or attacks, has become crucial for both the private and public sectors. Ensuring an adequate level of functionality during emergencies, such as disasters, is also a priority, which can be attained by enhancing infrastructure resilience. Resilience metrics and models play a significant role in understanding the complex interplay between the behaviors and operational characteristics of interdependent critical infrastructures. Additionally, these models and metrics must demonstrate the interdependencies among infrastructures to provide a more comprehensive representation of infrastructure resilience. This paper reviews, categorizes, and presents resilience metrics and models for Smart Interdependent Critical Infrastructures (Smart ICIs). This paper provides a comprehensive evaluation of various resilience models and measurements tailored specifically for interdependent critical smart infrastructures. It includes the essential terminology and definitions related to the resilience of Smart ICIs, investigates the universally recognized phases and capabilities of resilience, and examines the various types of failures that could potentially affect Smart ICIs.

Keywords: infrastructure systems; interdependencies; resilience assessment; smart infrastructures

Citation: Almaleh, A. Measuring Resilience in Smart Infrastructures: A Comprehensive Review of Metrics and Methods. *Appl. Sci.* **2023**, *13*, 6452. https://doi.org/10.3390/app13116452

Academic Editor: Chin Leo

Received: 17 April 2023
Revised: 13 May 2023
Accepted: 22 May 2023
Published: 25 May 2023

1. Introduction

With the continued growth of urban populations, the concept of resilience has become increasingly central to the sustainability and functionality of our cities. It is imperative to fortify our urban environments with resilience strategies to ensure their ability to adapt, recover, and thrive amidst the diverse challenges accompanying dense population centers, including environmental, social, and infrastructural stresses [1]. Over the past several decades, the proportion of the global population residing in urban areas has grown from 33% to 55% [2]. This rapid urbanization has exerted immense pressure on infrastructures that provide essential city services, leading to a surge of interest in developing smart cities. Smart city initiatives aim to establish intelligent, data-driven urban infrastructures by leveraging advancements in data analytics and information and communication technology (ICT) to enhance functionality, performance, and sustainability. In the context of today's society, it is important to highlight the difficulties encountered by interdependent smart critical infrastructures, especially when taking into account the differences between urban and rural settings. Smart infrastructures are especially useful in metropolitan areas due to the high population density and level of technological integration found there. These adaptive and interdependent systems can increase resistance to shocks and improve productivity under pressure.

However, in rural settings, the picture can be drastically different. These regions typically lack the extensive, dense networks observed in cities, and their infrastructures may be less technologically advanced. Due to this discrepancy, critical infrastructures may become less dependent on one another, which could compromise the system's overall

resilience. It can also be difficult to implement smart technologies in these settings due to a lack of resources (both financial and technical). To achieve this goal of balanced and equitable resilience, it is essential to take into account the different requirements and resources of urban and rural areas during the planning, design, and implementation of smart interdependent critical infrastructures. In reference [3], the authors define a smart city as "an urban region that employs various electronic data collection sensors to generate information, which is then utilized to manage assets and resources effectively. This encompasses data gathered from citizens, devices, and assets that are processed and analyzed to monitor and control traffic and transportation systems, power plants, water supply networks, waste management, law enforcement, information systems, schools, libraries, hospitals, and other community services".

The core principle behind the implementation of a smart city involves the seamless integration of physical infrastructure, information and communication technology (ICT) infrastructure, social infrastructure, and business infrastructure to bolster the collective intelligence of a city [4]. Smart city infrastructure encompasses physical, digital, and electrical backbones, including transportation networks, telecommunication networks, traffic light systems, streetlight systems, water treatment systems, gas supply systems, and power supply systems. ICT lies at the heart of these smart systems, transforming the physical infrastructure into intelligent entities [5].

Innovations in sensor technology, telecommunication infrastructures, control systems, cyber-physical operations, data management, and analytics are paving the way for smart infrastructures in cities, enhancing sustainability, efficiency, and residents' quality of life. For instance, in China, Shenzhen's citizens now enjoy a higher standard of living thanks to the deployment of resilient urban design and infrastructure that has improved the city's air quality, decreased traffic, and increased the dependability of its public transportation systems [6]. Policymakers and urban planners should prioritize initiatives that not only boost the city's infrastructures but also enhance the general living circumstances and happiness of its population by recognizing the influence of urban resilience on residents' well-being. Numerous smart city initiatives and projects have emerged in areas such as energy efficiency, transportation management, environmental monitoring, and asset management [5,7]. Unique trends are observable in deploying smart water infrastructure and utilizing wireless sensors and actuators connected to nearby water distribution networks to monitor various operations, including pressure, leaks, ruptures, water quality, traffic management, and public transportation within smart transportation networks [8].

It is important to note that these new smart infrastructures are increasingly interdependent [9], particularly the integration of electrical power and ICT. This interdependence creates various vulnerabilities to both external and internal forces. External forces encompass natural disasters and extreme weather events (e.g., hurricanes, tornadoes, wind storms, ice storms), while internal forces include failures resulting from component malfunctions, system breakdowns, and human errors. This type of interdependence between smart infrastructures is referred to as "Smart Interdependent Critical Infrastructures (Smart ICIs) [10]". In this context, the primary focus of this paper is to elucidate the concept of resilience within the realm of Smart ICIs and to showcase the diverse resilience metrics and methodologies that researchers employ to evaluate the resilience of Smart ICIs.

The idea of resilience is examined in this research in relation to Smart Interdependent Critical Infrastructures (Smart ICIs) [11], which are becoming more and more crucial to the operation of smart cities. These infrastructures are more vulnerable to different internal and external pressures, including natural disasters, component failures, and human error, as they become more linked. The study analyzes various resilience metrics and approaches that academics use to evaluate and improve the resilience of Smart ICIs in order to address these issues. The paper seeks to offer insights into the most efficient methods for enhancing the robustness and adaptability of these crucial urban systems, assuring their continued operation and ability to survive interruptions. These approaches cover a wide range of methodologies, such as simulation, network analysis, mathematical modeling, and

empirical evaluations. The picture emphasizes the benefits and drawbacks of each approach, providing helpful insights into how well-suited each is to various types of Smart ICIs and particular resilience concerns. This thorough knowledge of the state of the art in resilience measurement can aid practitioners and decision makers in creating more effective plans for boosting the resilience of their urban systems, ensuring the sustainable growth of smart cities in a society that is becoming more interconnected.

The trend in measuring the resilience of intelligent infrastructure is toward more integrated and holistic approaches. This transition is primarily motivated by the realization that smart infrastructures are interdependent systems in which a disruption in one component can have cascading effects [12] throughout the entire network. Consequently, the traditional, isolated method of measuring resilience is being supplanted with methods that can capture these interdependencies. In addition, there is a greater emphasis on dynamic resilience metrics that take into consideration the adaptability of these systems in response to changing conditions and threats [13]. Data analytics and artificial intelligence advancements play a crucial role in this trend, enabling more sophisticated models that can process large quantities of data and generate more precise and actionable insights [14]. In addition, there is a growing interest in developing resilience metrics that assess not only the technical aspects of smart infrastructures, but also the social, economic, and environmental dimensions. This reflects a larger transition toward a more sustainable and resilient infrastructure development and management strategy.

This paper is structured as follows: Section 2 presents an overview of the resilience of Smart ICI. Definitions, aspects, and perspectives relevant to ICI are included in Section 3. Resilience metrics and models for ICI, which experts implemented to assess the resilience of ICI, are presented in Section 4. The concluding remarks and future challenges relevant to this work are presented in Section 6.

2. Critical Infrastructures (CIs)

Critical infrastructure, as defined by [15], encompasses systems that consist of industries, organizations, and distribution capabilities that provide a continuous flow of essential services vital to the defense and economic security of society. These systems are often referred to as lifeline systems. Critical infrastructure incorporates various systems such as electric power systems, telecommunications, water treatment and supply, natural gas supply, transportation systems, and healthcare systems [16]. These infrastructures do not exist independently; instead, they are interconnected, giving rise to the term "interdependent critical infrastructures" (ICI). ICIs encompass all interconnected critical infrastructures utilizing different connection models, such as physical, geographical, cyber, and virtual connections.

The interconnected nature of ICIs amplifies the need for a comprehensive understanding of how these infrastructures interact with each other. This understanding can help identify potential vulnerabilities and risks associated with their interdependence. In turn, this awareness can lead to the development of more resilient systems that can withstand various threats and maintain their functionality during crises or emergency situations.

Moreover, as the world moves towards an increasingly digitized and connected environment, the interdependence of critical infrastructures becomes even more pronounced. This shift creates new challenges and opportunities for enhancing the resilience of these interconnected systems. By developing robust and adaptable resilience metrics and models, stakeholders can better manage and mitigate the potential impacts of disruptions on critical infrastructures, thereby ensuring the rapid recovery of essential services and the well-being of society as a whole.

2.1. Smart Interdependent Critical Infrastructures (ICIs)

Interdependence is an interdependence between two infrastructures in which the operational effectiveness of one is intrinsically linked to the performance of the other. Consider the electric power network and the natural gas network, for instance. The

preponderance of electric power generators relies on natural gas as a fuel source, while certain components of the natural gas infrastructure, such as compressors, require electricity to function. In such a scenario, any disruption to the electrical power grid may cause a disruption in the natural gas network. In contrast, a decrease in natural gas pressure could hinder power generation. Smart Interdependent Critical Infrastructures (Smart ICIs) adhere to the same interdependence principle as traditional ICIs. However, the incorporation of advanced Information and Communication Technology (ICT) could substantially amplify their interdependence [17–19].

Infrastructure interdependencies are more than just theoretical concerns. Numerous policy reports have recognized the importance of understanding the relationships between infrastructures [20]. These reports highlight the growing attention at the governmental policy level toward the significance of incorporating interdependencies in national strategies to protect and defend critical infrastructures. While infrastructure service providers possess extensive experience in responding to and mitigating blackouts or minor disruptions, there is a crucial need for the nation to prepare for and recover from critical interruptions which may arise due to terrorist attacks or natural disasters.

Furthermore, as the world becomes more interconnected and digitized, the complexities of smart interdependent critical infrastructures continue to evolve. This progression necessitates continuous advancements in the development of resilience metrics and models to understand and manage the potential impacts of disruptions on these interconnected systems. By enhancing the resilience of Smart ICIs, stakeholders can better safeguard the essential services that these infrastructures provide, ensuring the continuity of these services and the well-being of society as a whole.

2.2. Interdependence Types

Smart ICIs exhibit various types of dependencies and interdependencies. While dependency refers to a unidirectional connection between infrastructures, interdependency implies a bidirectional relationship between them [21]. Numerous scholars have categorized the interdependencies between infrastructures in different ways [22].

In addition to these primary types of interdependencies, it is essential to consider the potential cascading effects that can occur within and between interconnected infrastructures. As the complexity of Smart ICIs increases with the integration of advanced technologies, the possibility of cascading failures across multiple systems becomes a pressing concern. Identifying and understanding the different types of interdependencies can help policymakers, planners, and infrastructure managers develop more effective strategies to mitigate the risks associated with these complex relationships and enhance the resilience of Smart ICIs.

Moreover, the increased interconnectivity and digitization of Smart ICIs bring both opportunities and challenges. On the one hand, interdependent infrastructures can improve efficiency, resource optimization, and better decision making. On the other hand, the growing complexity of these systems can make them more vulnerable to disruptions, cyberattacks, and other potential threats. Therefore, it is crucial for stakeholders to strike a balance between leveraging the benefits of interdependent critical infrastructures and addressing the challenges they pose. This can be achieved through continuous research, innovation, and collaboration among various sectors, ultimately contributing to a more resilient and sustainable society; however, in this paper, we classify the interdependencies in critical infrastructures into five primary types:

- **Physical Interdependence:** Infrastructures exhibit physical interdependence when the functioning of one infrastructure relies on the physical output(s) of another. For example, consider the relationship between a coal-fired power generation plant and its associated railroad system. The power plant generates electricity, which serves as an input for maintaining the railroad control center's operations. Simultaneously, the railroad system is responsible for transporting coal to the power plant, ensuring its fuel supply. In this case, the physical interdependency connection is established through

the electricity produced by the power plant and its role in sustaining the railroad system's services. The physical dependence of the renewable energy infrastructure on various factors adds another layer of complexity. For instance, wind turbines are susceptible to changes in wind speed and direction, solar panels depend on sunlight intensity, and hydroelectric systems are reliant on water flow rates. Any disruptions in these physical dependencies can significantly impact the power generation and, in turn, the resilience of the entire system [23].

This underscores the need for an integrative approach to resilience, encompassing not only technical considerations but also the physical dependencies of renewable energy infrastructures. Ensuring resilience in this context requires a thorough understanding of these dependencies and the development of strategies to manage potential disruptions. This might include the diversification of renewable energy sources, strategic placement and design of infrastructure to withstand environmental stresses, and the implementation of systems that can quickly adapt and respond to changes in renewable energy supply.

- **Logical Interdependence:** Infrastructures demonstrate logical interdependence when the functioning of one system depends on the functioning of others through a mechanism that is not connected to physical, cyber, or geographic factors. For instance, power system outages can lead to fluctuations in the prices of food and fuel. In this case, the relationship between the infrastructures is established through a logical connection, rather than a direct physical, cyber, or geographic link.
- **Cyber Interdependence:** Cyber interdependence manifests between infrastructures when they are directly linked via an information exchange within an informational infrastructure. This form of interdependency connects critical infrastructures through informational pathways, where one infrastructure's output data serves as another's input. Such an exchange between infrastructure systems must inherently involve data transfer. Consider, for example, the typical operation of communication systems, which depends on the electrical power generated by power plants and distributed via transmission systems. To guide this electricity to the required systems, a Supervisory Control and Data Acquisition (SCADA) system is utilized to administer the electric power networks. The SCADA system leverages communication systems to send and collect information from diverse power sectors, thus establishing a cyber interdependency nexus between the power and communication systems.
- **Geographic Interdependence:** Geographic interdependence occurs when multiple infrastructure systems are situated within the same local area, which can result in functional changes to all systems involved in the event of a disruption [24]. For example, during the 9/11 attack on the World Trade Center, the collapse of the buildings caused functional disruptions to water systems, rail tunnels, a passenger station, and one of the world's largest telecommunication nodes [22].
- **Social Interdependence:** Social interdependence arises when the connection between two smart interdependent infrastructures is partially rooted in human behavior outcomes. Healthcare and other critical infrastructures are not standalone operations; rather, they are embedded in a vast network of interdependent structures. Their operation and effectiveness are heavily reliant on the proper functioning of other critical infrastructures, demonstrating their intricate interdependence. For instance, healthcare systems depend on the reliable supply of electricity for life-supporting equipment, telecommunication networks for data transmission and coordination, transportation systems for the mobility of patients and staff, and water systems for sanitation and hygiene.

  When a disruption occurs in any of these supporting infrastructures, it can have a profound impact on the healthcare system. For example, a power outage can incapacitate essential medical equipment, compromising patient care and even leading to loss of life in extreme cases. Similarly, a failure in the transportation system might prevent patients from reaching hospitals or delay the delivery of critical medical

supplies. This is where the social interdependence between these systems becomes apparent. The community relies on these interdependent infrastructures for their health and well-being. Disruptions can not only affect physical health but also cause stress and anxiety, impacting the community's overall social and mental well-being. Thus, the resilience of one infrastructure directly influences the resilience of others and in turn, the resilience of the society they serve. It underscores the need for a holistic, system-of-systems approach to resilience planning, ensuring that each infrastructure can withstand, adapt to, and recover from disruptions, thereby safeguarding the community's health and wellbeing.

2.3. Failure Types

The various types of failures that arise from dependencies due to disruptions are grouped into distinct categories, which encompass cascading, escalating, and common-cause failures. These classifications are essential in understanding how the dependencies affect the functioning of interdependent infrastructures when faced with disruptions. By evaluating and categorizing these failures, researchers and practitioners can better identify the most effective strategies for mitigating their impact and enhancing the resilience of interconnected systems. Furthermore, this classification allows for a more accurate assessment of the potential risks and vulnerabilities associated with each type of failure, leading to more informed decision making in managing and protecting these vital infrastructures. Overall, understanding the different types of failures is crucial in developing comprehensive and robust strategies to ensure the stability and sustainability of interdependent critical infrastructures [21]:

- **Cascading failure** is characterized as a situation where a disruption in one infrastructure (Infrastructure A) impacts one or more elements within another infrastructure (Infrastructure B), consequently leading to partial or total unavailability of Infrastructure B. An example of this type of failure is when an electrical power outage affects communication systems, causing disruptions or a complete loss of connectivity in those systems [25].
- **Escalating failure** is defined as a situation in which a disruption in one infrastructure exacerbates an independent disruption in another infrastructure, typically by increasing the severity of the functional loss or prolonging the recovery or repair time for the second infrastructure. For example, a disruption in an ICT system may amplify the impact of a separate disturbance in a road transport system, leading to more significant consequences or longer restoration times.
- **Common-cause failure** happens when two or more infrastructure systems experience a disruption simultaneously due to a single underlying cause. This could be because the infrastructures are physically located in close proximity and depend on shared resources, such as power or communication lines. Alternatively, it could be due to an external factor that impacts multiple systems at once, such as a natural disaster. When such failures occur, it can be challenging to manage and recover from as it affects several systems simultaneously and requires a coordinated response from various organizations. For example, if a natural disaster hits an area, it could lead to the failure of all physical infrastructures in that region, thereby causing significant disruptions.

3. Resilience

Resilience has recently emerged as a theoretical framework for examining and assessing an infrastructure's performance prior to, during, and following the occurrence of a disturbance. Such disturbances could arise from natural hazards or mechanical and technical failures. Moreover, resilience is being increasingly recognized as a proactive approach aimed at bolstering the robustness of infrastructures to enhance their preventative, mitigative, and recovery capabilities in the face of disruptive events [26].

Resilience is a concept defined in various ways, often contingent on the context of the analysis, whether it is an asset, a facility, a system, or a system-of-systems. In this discussion,

we concentrate on definitions that pertain to the system-of-system or interdependent systems. One such definition posits resilience as "the capacity of a system to absorb disturbance, undergo change, and retain essentially the same function, structure, identity, and feedback" [27]. This perspective primarily focuses on resilience in the aftermath of a disruptive event.

A contrasting definition proposed by the US government encompasses resilience both prior to and following an event, as depicted in Figure 1. It defines resilience as "the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies" [28]. The Department of Homeland Security (DHS) offers a more specific definition of resilience in the context of critical infrastructures: "the ability to reduce the magnitude, impact, or duration of a disruption. Resilience is the ability to absorb, adapt to, and rapidly recuperate from a potentially disruptive event" [29].

Furthermore, a smart city can be considered resilient to a certain degree if it has enhanced capabilities to absorb anticipated shocks and strains to its social and technical network and infrastructures while maintaining the necessary level of functions, structures, and identification.

Resilience has become a central concept for identifying and evaluating the performance of infrastructures before, during, and after a disturbance. These disturbances could be the result of natural calamities or mechanical or technological failures. As a forward-thinking strategy, resilience has garnered a great deal of attention for its potential to fortify infrastructure and improve its prevention, mitigation, and recovery capabilities during an event.

There are numerous definitions of resilience, the particulars of which are frequently dependent on the context of analysis, such as whether it pertains to an asset, facility, system, or system-of-systems. The concentration of this article is on definitions pertinent to interdependent systems or system-of-systems. According to [27], resilience is "the capacity of a system to absorb disturbance, undergo change, and retain essentially the same function, structure, identity, and feedback". This explanation emphasizes the resilience following a disruptive event.

In contrast, the US government's proposed definition includes resilience both before and after an event. It defines resilience as "the ability to adapt to changing conditions and endure and recover quickly from disruptions caused by emergencies" [28]. The Department of Homeland Security (DHS) offers a more detailed definition of resilience in relation to critical infrastructures. According to them, resilience is "the capacity to lessen the extent, impact, or duration of a disturbance [29]". Resilience is the capacity to absorb, adapt to, and swiftly recover from a potentially disruptive event.

The American Society of Civil Engineers (ASCE) FEMA P-58 code [30], known as the Seismic Performance Assessment of Buildings, provides a vital framework for evaluating a building's potential seismic performance. This robust methodology is integral to the design for resilience, providing a performance-based approach that allows for detailed estimations of potential losses due to seismic events. The comprehensive nature of the FEMA P-58 code extends beyond assessing structural damages to encompass non-structural components, casualties, repair costs, and repair time.

By estimating the total potential impacts—including downtime, loss of functionality, and economic implications— this methodology equips engineers with the necessary tools to design structures that are not only resistant to seismic events but also capable of a faster recovery. Implementing FEMA P-58 code is thus crucial in ensuring the resilience of critical infrastructures, as it allows for a holistic understanding of how these infrastructures would fare and recover in the event of a seismic disturbance.

In addition, a smart city is resilient if it is supplied with safeguards to effectively absorb potential shocks and stresses to its social and technical networks and infrastructures. This resiliency enables it to maintain the requisite levels of function, structure, and identification despite stress.

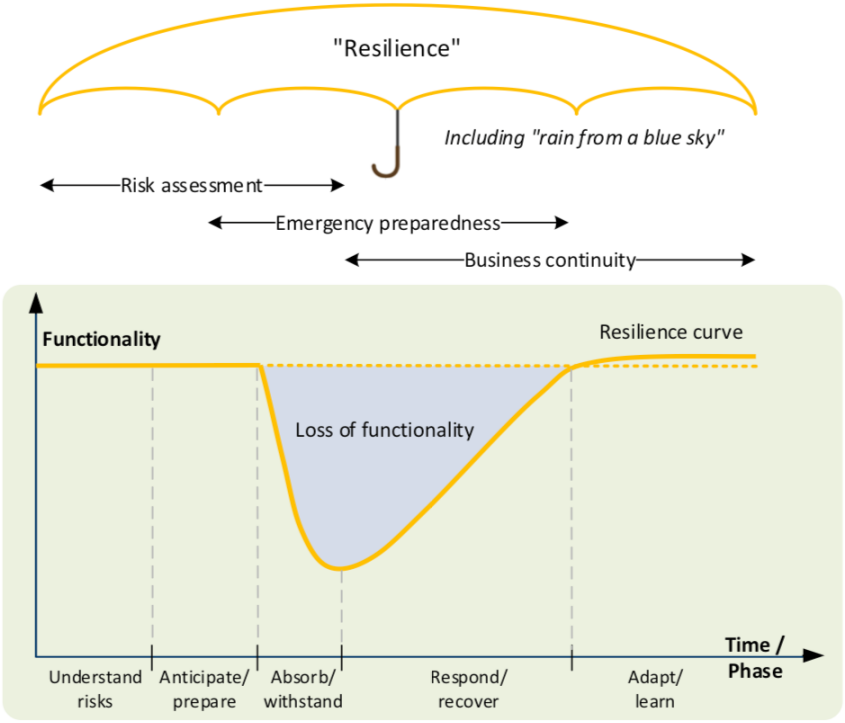

Figure 1. Resilience Umbrella [31].

3.1. Resilience in Smart ICI

The resilience of contemporary societies is fundamentally intertwined with the resilience of their Critical Infrastructures (CIs). The National Infrastructure Advisory Council (NIAC) [16] has aptly defined infrastructure resilience as "the ability to lessen the intensity, impact, or duration of a disruption, absorb and adapt to the disruption, and promptly recover from a potentially disruptive event". It is incumbent upon critical infrastructure resilience to develop a strategy that is self-sufficient but can also contribute to the calculation of other measures, given its role as an element of community and regional resilience, which includes the resilience of social, economic, and other subsystems.

The SmartResilience project [32] characterizes the resilience of infrastructure as "the capability to foresee potential adverse scenarios or events (including new or emerging threats) that could disrupt the operation or functionality of the infrastructure, prepare for them, withstand or absorb their impacts, recover from the disruptions they cause, and adapt to changing conditions" [32]. An infrastructure is generally deemed smarter when it exhibits greater innovation in regular operations.

Moreover, smarter infrastructures often display the following attributes: they are integrative and interdependent, innovative through the adoption of Information and Communication Technology (ICT), they utilize web technology, implement smart computing, are oriented towards smart governance, are sustainable, progressive, future-oriented, and have practical settings. However, it remains to be observed whether such a smart critical infrastructure (Smart ICI) would rebound "smartly" or exhibit "smart resilience" when confronted with severe threats, such as extreme weather events or terrorist attacks.

Furthermore, one of the key questions scientists have been grappling with recently is whether making our current infrastructure smarter might inadvertently increase its vulnerability. Could this transformation affect the resilience of a Smart ICI in its ability to anticipate, prepare for, adapt and withstand, respond to, and recover from disruptive events? While risk analysis has been touted as a vital tool in disaster scenarios, it differs from resilience in that it is more closely tied to the identification and analysis of potential events that could have a negative impact on individuals, assets, and the environment.

This is accomplished by conducting a risk assessment at a given time to measure the vulnerabilities of the systems.

Smart Community-based resilience is another vital perspective that underscores the importance of local communities in managing and reacting to various types of crises, such as natural disasters, economic shocks, and social disruptions. This perspective suggests that communities possess unique insights, abilities, and resources that can be utilized to strengthen their capacity to resist and recover from these crises [33]. The concept of community-based resilience [34] encompasses enhancing social cohesion, fostering local leadership, cultivating collective efficacy, and providing psychosocial support, among other factors [35]. By involving community members in decision-making processes and resilience-building initiatives, this approach aims to foster more sustainable and equitable solutions. In 2010, Argonne National Laboratory, in collaboration with the DHS Protective Security Coordination Division, designed a measure of the resilience of smart critical infrastructure [36]. The Resilience Index (RI) was based on the method recommended by the National Infrastructure Advisory Council, which argued for analyzing the resilience of an organization or system by recognizing three essential components: robustness, resourcefulness, and rapid recovery. Briefly stated, the RI was constructed from data collected via the Infrastructure Survey Tool (IST), which was adjusted to address different forms of robustness, resourcefulness, and rapid recovery. Additional detail on the IST is given in Section 4. Since resilience is a multifaceted concept, it is crucial to evaluate resilience within the context of interest. The context of this paper is smart interdependent critical infrastructure systems, such as power networks, water networks, and health facilities, with a particular interest in disaster response operations. All the above definitions for resilience indicate how the system should be designed to protect an individual infrastructure from any disturbance event that could lead to a failure in the system functionality. The exact definition applies to the resilience of the interdependent infrastructure. That can be accomplished by expanding the protection from a single working infrastructure into n numbers of infrastructures that run simultaneously with interdependent functionality.

3.2. Disturbance Event Phases

Resilience evaluation is indispensable for decision support, aiming to quantify the efficacy of preparedness expenses and plans. A practical preparedness blueprint enhances the stability of critical infrastructure in the wake of a disruptive event. Numerous models and measures have been devised to gauge the performance and service of smart systems, aiding in the design, upkeep, and enhancement of overall resilience. Nevertheless, resilience is a complex concept, challenging to tackle by examining just one specific capability. A comprehensive approach to tackle the intricacies of resilience necessitates the creation of sophisticated measures that scrutinize key resilience characteristics—primarily absorptive, adaptive, and restorative capabilities. These attributes must be evaluated in the context of different phases of a disruptive event, considering the unique conditions and challenges each phase presents.

Each assessed attribute represents a component of the system's response to disruptions, offering insights into its ability to absorb shock, adapt to changing conditions, and restore its functionality. Once these assessments are made, they can be synthesized into a singular, unified resilience metric that encapsulates the system's overall resilience. The refinement of this unified resilience metric can be further achieved by transitioning the phases of disturbance events into weighted points. This process allows the contribution of each phase to the overall resilience to be quantified and compared. Such a method facilitates independent experts in delineating estimates for limit values, thereby adding an additional layer of precision to the resilience metric.

This comprehensive and robust resilience metric not only encapsulates the system's resilience across various phases of a disruptive event but also provides a quantifiable means to compare and improve resilience across different systems or configurations. Thus, it serves as a crucial tool for decision makers in enhancing the resilience of critical infrastructures.

- **Risk comprehension:** Applicable prior to the adverse event, this phase underscores potential emerging risks (ERs) and involves early detection. For example, what might the *adverse event* entail? How can we gather more information and context about the risk or hazards?
- **Anticipation and preparation:** This phase involves devising preparation and proactive evolution plans. For instance, what outcomes should we anticipate?
- **Absorptive capacity/withstand:** Absorptive capacity pertains to the system's ability to mitigate the negative implications caused by disruptive events and minimize their impact. An exemplification of this phase is enhancing robustness to improve system redundancy, which offers an alternate means for the system to operate.
- **Restorative capacity/recovery:** Restorative capacity concerns the infrastructure's ability to be enhanced by external interventions during the recovery period. For instance, implementing real-time monitoring operations (e.g., Supervisory Control and Data Acquisition system or SCADA for most infrastructures) bolsters the infrastructure's restorative capability. It allows for the automated detection of disruptive events, which is crucial in minimizing the total disruption time.
- **Absorption/withstand:** This phase corresponds to the actions during the initial phase of the event and should include vulnerability analysis and potential consequences. For example, how steep is the absorption curve and how far below will it dip?
- **Adaptation/learning:** Adaptive capacity refers to the infrastructure's ability to adjust to disruptive events within its self-organization skills to minimize outcomes. It represents the remarkable ability of the infrastructure to improve itself during the recovery period.

Several approaches to quantify resilience have been introduced recently. In 2003, An initial framework was proposed to include the seismic resilience of society [37] by presenting the theory of *Resilience Loss*, later referred to as the resilience triangle. Figure 1 plots an example of the concept of resilience phases and also shows the resilience triangle, where the figure determines the property or functionality and the overall infrastructure performance after around a half function loss. The resilience triangle depicted in the figure represents the loss of functionality due to a disruptive event and the process of restoration and recovery over time. The fundamental objective of resilience-enhancing metrics is to shrink the area of the resilience triangle. This is achieved by implementing various strategies to boost the functionality and performance of the infrastructure (represented by the vertical axis in the figure), thereby reducing the recovery time. For instance, mitigation measures can be employed to augment infrastructure performance and trim down recovery time. Furthermore, the time needed for recovery can be expedited by enhancing measures for the restoration and replacement of impaired infrastructure.

4. Current Approaches to Measure Resilience in Smart ICI

Smart Interdependent Critical Infrastructures (Smart ICIs) currently employ a variety of methods for measuring their resilience. In general, these methods can be categorized as qualitative or quantitative. To evaluate resilience, qualitative methods frequently employ expert opinions, surveys, and conceptual models, whereas quantitative methods employ mathematical and statistical models. Typical resilience measurement indicators include robustness, redundancy, resourcefulness, and speed. These indicators are used to evaluate the system's ability to withstand disruptions, recover rapidly, and adapt to changing conditions. Developing a resilience index that incorporates these various indicators is a common strategy. Given the complexity and interdependence of Smart ICIs, however, there is a growing emphasis on the development of more sophisticated and comprehensive models that can capture these interdependencies and provide a more accurate and holistic assessment of resilience.

In terms of methodology, as shown in Figure 2, a systematic literature review approach was utilized for this review paper. This required a literature review on the topic of resilience in Smart ICIs, as illustrated in the figure below. Using a combination of keyword searches

and citation monitoring, relevant articles from various databases, such as academic journals, conference proceedings, and technical reports, were identified. The selected papers were then subjected to a comprehensive analysis to extract pertinent information and insights. The review process was iterative, with the search strategy being modified based on the results of the initial literature review. The information gleaned from the literature was then synthesized and classified according to the various examined aspects of resilience, such as definitions, models, metrics, and strategies. This methodical and exhaustive approach ensured that the review captured the scope and depth of current research on this crucial topic.

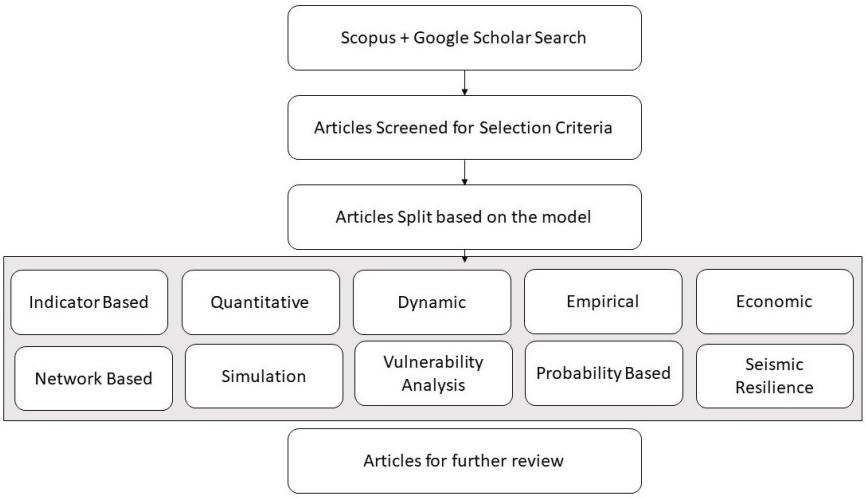

Figure 2. Review Methodology [38].

4.1. Indicator-Based Approach

The indicator-based approach is a widely used method for measuring resilience at a global level. It involves establishing specific indicators and threshold values to determine the resilience of infrastructure systems. By setting appropriate indicator levels, this approach can provide a quantitative assessment of resilience for different types of infrastructure.

4.1.1. The ANL Method

A notable example of an indicator-based methodology for assessing resilience is the resilience index (RI) developed by Argonne National Laboratory. This approach utilizes uniform and consistent data, initially gathered through a revised report from the US Department of Homeland Security (DHS) Enhanced Critical Infrastructure Protection (ECIP) plan [36]. The resilience measurement index (RMI) comprises three primary categories for determining overall resilience: robustness, resourcefulness, and recovery. The methodology is structured across five hierarchical levels, with indicators generated at the lowest level.

Resilience assessment involves inputting indicator values at level five and aggregating them up to the first level. The RI then evaluates the resilience level of critical infrastructures, ranking and prioritizing those with limited support to improve overall resilience. Equation (1) presents the fundamental mathematical model, which encompasses the sum of the three main components: robustness, resourcefulness, and recovery:

$$RI = \sum_{i=1}^{3} e_i * V_i \quad (1)$$

Here, RI represents the relative resilience index (ranging from 0 to 100); e_i is the scaling constant (weight; a number between 0 and 1) that indicates the relative importance of component $i(i = 1, 2, 3)$ of resilience; and V_i is the index value of component i of resilience (i.e., robustness, resourcefulness, and recovery). The index value of component

i is the aggregated value from level 1. However, in level 2, each component possesses sub-components. For instance, robustness contains three sub-components (redundancy, prevention, and maintaining key functions) in level 2, each with an index value representing the overall robustness value.

A similar structure is observed in level 3, wherein each sub-component is further divided into additional information layers. For example, redundancy in level 2 is a primary element of robustness (level 1) and comprises eight subcategories (electric power, natural gas, telecommunications, information technology, water, wastewater, transportation, and critical products). These subcategories are recognized in level 3 and are further divided into distinct components. In this case, the electric power category (level 4) consists of four subcategories (on-site backup generation, uninterrupted power system, internal generation, and connections). To scale level 4 components, such as electrical power connections, raw data (level 5) is collected from the facility's responses to personal questions, resulting in a cumulative value for electric connections.

4.1.2. The REWI Method

The Resilience-Based Early Warning Indicator (REWI) method [38] encompasses three primary components: contributing success factors (CSF), general issues, and indicators. The central element, contributing success factors (CSF), consists of attributes of resilience used to derive the overall rating of a specific infrastructure. CSFs comprise various components or factors, such as the *Risk Understanding* factor, which seeks to clarify questions such as how information and expertise about risk/hazards are obtained. *Anticipation* is another CSF component that addresses expectations prior to a disruptive event. *Attention* is a key factor determining which aspect of the infrastructure requires the most focus. *Response* is a crucial factor concentrating on the actions to be taken during the event. *Robustness (of response)* indicates the approach to ensure the accomplishment of response factors with minimal damage. *Resourcefulness/rapidity* denotes indicators that ensure timely reactions to the event. *Decision support* is another critical factor suggesting the need for an indicator that elucidates the trade-off between safety and production. *Redundancy* is the final primary factor related to the CSFs indicators, which addresses strategies used to compensate for the unavailability of critical infrastructures.

The second component of the *REWI* method involves common issues for each contributing success factor (CSF), ensuring that the objective of each CSF is met. For instance, the first CSF (Risk Understanding) has several issues to address, such as system knowledge and reporting of incidents, near-misses, and accidents. The third and final component of the *REWI* approach is the indicators, which are assigned to each general issue component and illustrate the process of assessing general issues.

4.1.3. The SmartResilience RIL Method

Similar to the REWI method, the Smart Resilience Level (RIL) [39] method employs *issues* and *indicators* at the two lowest levels of the structure, while *phases* are utilized at the next higher level, as opposed to themes in LIOH and contributing success factors in REWI. For each phase, significant issues are identified, guiding the implementation of indicators to evaluate these issues and assign estimation values accordingly. The hierarchical model comprises six distinct levels, as depicted in Figure 3.

The *RIL* method relies on character scores ranging from E to A, where A is the best and E is the worst, assigned to each level. Furthermore, each score is associated with a weighted value corresponding to a specific resilience level (RIL). For instance, a weighted value score between 0–1 corresponds to level E, while a weighted value between 1–2 signifies resilience level D, and so on. The quantification process of the method involves initially selecting the area of interest, such as a smart city. Subsequently, specific smart ICI components within the area must be chosen, along with identifying the most relevant threats for each SCI. The next step requires considering each phase of the event for every threat and determining the issues within each phase. A comprehensive investigation of the indicators for each issue

should be conducted, followed by defining the range values for each indicator. Finally, values are assigned to the indicators, and the overall *RIL* calculations are completed. This approach primarily aims to measure *preparedness* to identify potential issues before they arise.

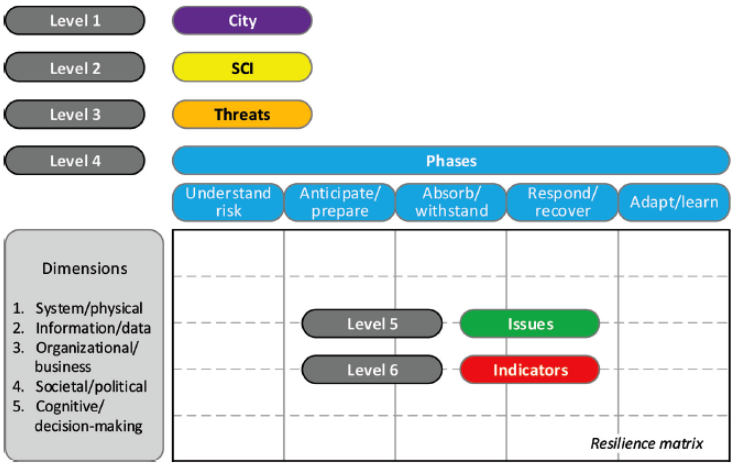

Figure 3. The six levels in the hierarchical model [38].

4.1.4. DHS Infrastructure Survey Tool

In 2009, the US Department of Homeland Security began using questionnaires to evaluate the resilience of critical infrastructure. The Infrastructure Survey Tool (IST) is one of the most widely employed questionnaire tools, functioning as an indicator-based method that assesses individual protective measures and vulnerability within the protective measure and vulnerability indices (PMI/VI). The IST was enhanced to serve as a resilience measure by developing a comprehensive methodology that applies uniform and consistent data to generate a resilience index (RI). The *RI* value is derived from three components: robustness, resourcefulness, and recovery. The *RI* has a value range between 0 and 100, where 0 indicates the lowest resilience [40]. The *RI* leverages the results of this tool to compare resilience levels across smart critical infrastructure sites.

Upon calculating the *RI* for each component, an advanced resilience index is presented in the form of a dashboard. Figure 4 illustrates an example of the DHS dashboard, displaying the resilience index at the component level. The bar mark represents the observed infrastructure, while the low, average, and large dots indicate the comparative value in relation to other smart infrastructures. The implementation of this approach and its transparent representation enables facility administrators to make informed decisions more easily.

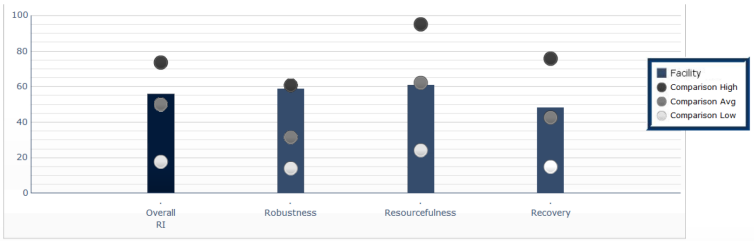

Figure 4. Dashboard displaying values of Resilience Indicator components for a sample facility [40].

4.1.5. All Hazards Knowledge Framework (AHA)

The primary motivation behind developing the AHA [41] was the need for a resilience tool capable of assessing the resilience of interdependent CI systems in an all-hazards context. The AHA is a framework that combines data and expert measures to calculate overall resilience. The AHA structure consists of three components: (1) facility-level dependency profiles; (2) dependency models; and (3) a text analysis system (TAS). Employing the

AHA tool enhances the decision-making experience by providing decision makers with the ability to comprehend critical dependencies, resilience, and the impacts of hazards on smart ICI.

Figure 5 illustrates the high-level deployment of the AHA tool, which employs a top-down approach. The process begins with identifying the region to be assessed and the aid sector service providers for that region. In the figure, the aid sector is represented by the blue rectangles in the middle row, followed by their critical infrastructures, depicted as orange squares. A significant electric generation station could be an example of such a case. Dark blue rectangles display the most critical dependencies between them. They propose a holistic approach to resilience that incorporates all resilience components. The Equation (2) presents a resilience measurement approach based on the AHA:

$$Res = f(aIR, bCR, cOR, dSR, ePR)|_r \quad (2)$$

where Res represents resilience; f denotes the function of; a, b, c, d, e, are scaling constants ranging from 0 to 1, based on the risk type being analyzed; r signifies risk, concerning interdependencies that may influence all risk elements; and $|_r$ is assessed at different levels of hazard. This equation asserts that resilience is a broad concept, formulated as a function of infrastructure resilience (IR), community resilience (CR), organizational resilience (OR), social resilience (SR), and personal resilience (PR). The weighting of each of these elements varies based on factors that change (geography, sector, scope, incident type, and time). Risk is a function of threat, vulnerability, and consequence that must be examined as a part of resilience assessment.

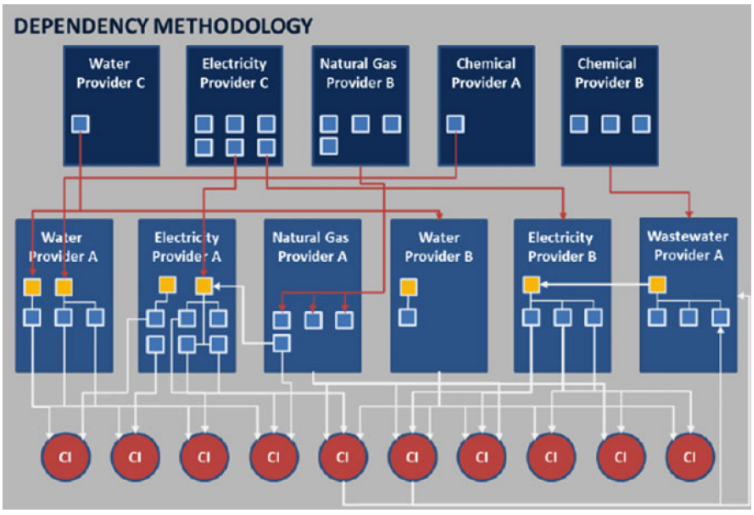

Figure 5. All Hazards Knowledge Framework dependency methodology [41].

Limitations: The primary drawback of this approach is that most models rely on judgmental data, which lacks accurate empirical information for determining resilience. Judgmental indicators result from expert questionnaires and the completion of indicators for each infrastructure. Indicators can only provide indications, not scientific proof or detailed explanations of change, partly because they are based on assumptions about system functionality, albeit informed assumptions.

4.2. Quantitative (Holistic) Approach

Quantitative methods can evaluate the resilience of any smart ICIs by encompassing the infrastructure's performance and functionality. Most of the quantitative models are employed to assess system resilience by comparing the operating performance in different event phases (before and after a disaster event). In the context of current resilience research concerning technical systems related to smart ICIs, there is a discernible shift from qualitative methods to quantitative models. Implementing these methods enables more accurate

resilience analysis, which can significantly contribute to this field. Several resilience metrics based on the quantification approach are presented as follows:

4.2.1. General Resilience (GR)

One of the most promising metrics presents an approach aimed at developing a mathematical model capable of examining the functionality of smart ICIs infrastructures. The primary objective is to generate a time-dependent method for estimating infrastructure resilience and utilizing the results for comparison purposes [42]. The outcomes of this method provide detailed analysis for decision makers, supporting improvements in infrastructure resilience; for example, estimating the priority of each phase of an infrastructure (i.e., the recovery phase) enables the more effective application of resilience strategies in that phase.

Measuring resilience is insufficient when analyzing an individual infrastructure's capability. As such, a unique model has been proposed that integrates various resilience capabilities (i.e., absorptive, adaptive, and restorative capability) across multiple phases (i.e., initial steady, disruptive, recovery, and new steady phase). This distinctive method can assess infrastructure performance over time based on system performance. To manage the progress of the unified resilience method, the representation of all infrastructures in Figure 6 is examined across four phases. Different approaches are used for each phase to reflect system performance, as summarized in Table 1. Subsequently, all values are combined into a single measurement of performance (MOP) value. This method, called General Resilience (GR), is represented as follows:

$$GR = f(R, RAPI_{DP}, RAPI_{RP}, TAPL, RA) = R * (\frac{RAPI_{RP}}{RAPI_{DP}}) * (TAPL)^{-1} * RA \quad (3)$$

As a case study for their model, the Swiss electric power supply system (EPSS) was selected as a representative application to demonstrate the utility of the suggested quantitative method. The case study will be discussed in greater detail in the next section.

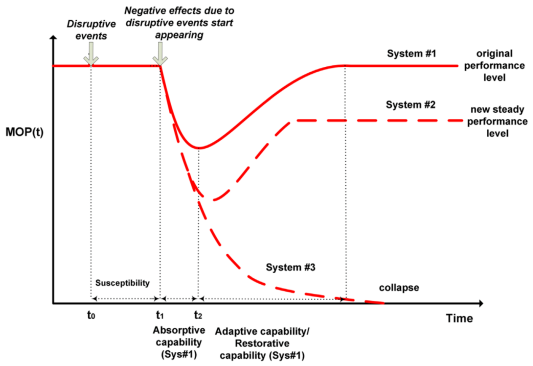

Figure 6. Illustration of essential resilience capabilities [42].

Table 1. Summary of different resilience phases [42].

Phase Measurements	Time Scope	Capabilities	Measurements
Original Steady phase	$t < t_D$	Susceptibility	Susceptibility
Disruptive Phase	$t_D \leq t < t_D$	Absorptive Capability	R $RAPI_{DP}$ PL_{DP}
Recovery Phase	$t_R \leq t < t_{NS}$	Adaptive Capability Restorative	$RAPI_{RP}$ PL_{RP}
New Steady Phase	$t \geq t_{NS}$	Recovery Capability	RA

4.2.2. Multi-Phase Resilience Trapezoid ($\phi\Lambda E\Pi$) or (FLEP)

An additional innovative resilience quantification framework to the GR metric is the Multi-Phase Resilience Trapezoid (MPRT) [43]. The FLEP approach focuses on developing a resilience trapezoid ($\phi\Lambda E\Pi$) that delineates various infrastructure timeline phases for smart ICIs. Figure 7 illustrates the multi-phase resilience trapezoid. This approach utilizes distinct indicators for each phase and aggregates them to represent the overall resilience for any infrastructure. By applying this approach, a precise estimation of resilience is provided, facilitating decision making for system functionality improvement.

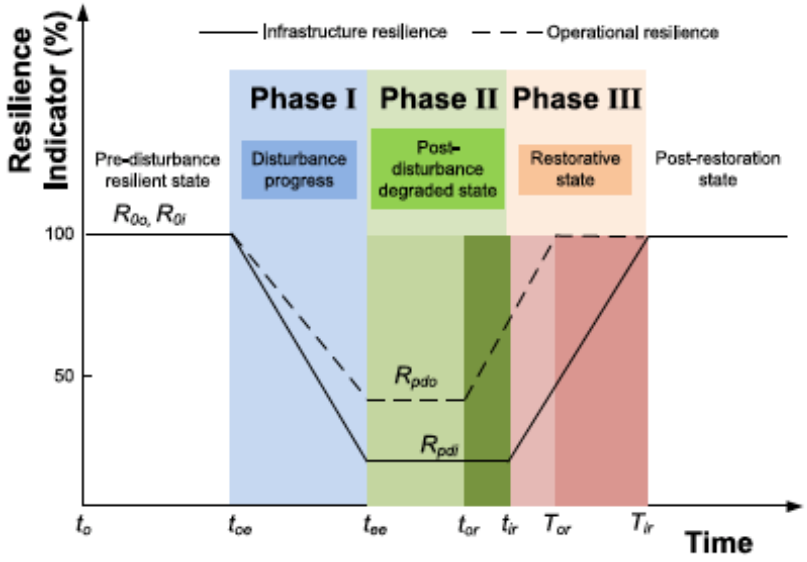

Figure 7. The multi-phase resilience [43].

The primary assumption of this model is that all the different indicators for the *pre-disturbance resilient state* (i.e., R_{0o} and R_{0i}, respectively) are 100% before the event occurs at t_{oe}, e.g., 100% of the demand for each user, and the transmission lines between them are online sequentially. The main four key resilience metrics are presented in Table 2, specifically addressing how active (ϕ) and how deep (Λ) the resilience declines in *Phase I*, the magnitude (E) of the post-event functionality loss situation in *Phase II*, and the speed (Π) at which the system recovers to its primary resilient state in *Phase III*. This collection, which includes four methods, is described as the resilience metric system ($\phi\Lambda E\Pi$) and is referred to as (FLEP).

Table 2. The ($\phi\Lambda E\Pi$) Resilience Metrics [43].

Phase	State	Resilience Metric	Symbol
I	Disturbance progress	How fast R drops? How low R drops?	ϕ Λ
II	Post-disturbance	How extensive is the post-disturbance degraded state?	E
III	Restorative	How promptly does the Network recover?	Π

4.2.3. QRMP

The Quantitative Resilience Management Tool [44] has been introduced by the RESILIENCE project [45], which encompasses a set of indices and characteristics (ICs) that are employed to describe and evaluate the infrastructure at both physical and operational levels. All measures related to the resilience project are categorized based on three event phases (before, during, and after). A set of weights captures the relative importance of

each IC. Upon collecting and aggregating the associated weight for each IC, the overall resilience scores can be identified, which include resilience at different timelines such as preparation, prevention and protection, response, and recovery. Moreover, this tool considers the resilience associated with each level (physical and operational). The Quantitative Resilience Management Tool can be divided into the following four steps to assess the overall resilience, as shown in Figure 8, which displays the input entries for each phase (previous, during, and after disaster). The columns illustrate the different system levels:

Definition of the structure of indices and characteristics (ICs) of the infrastructure. The most significant IC that can optimally represent the infrastructure must be identified, and based on that, each stage of the level receives a corresponding rank. This ranking and classification occur during this phase. For example, let $L = 1, 2, 3$ and $S = 1, 2, 3$ denote the level and the stage sequentially. Next, there will be $N_{L,}S_IC_s$ associated with every L, S pair, denoted by $IC = (IC_L^i, S, i \in N_{L,S})$.

1. Description of the table of weights. The weights associated with each IC are expressed as $W = W_{L,}^i S, i \in N_{L,S}$. It is stated that the weights have to be selected, such that:

$$\sum_{i=1...N_{L,S}} W^i{}_{L,S} = 1 \tag{4}$$

2. Statistical representation of the ICs.
3. Obtaining the resilience sums. The expression provides the resilience scores corresponding to each L, S pair:

$$R_{L,}S = \frac{1}{N_{L,S}} \sum i = 1...N_{L,S} W_{L,S}^i \, IC_{L,S}^i \tag{5}$$

The resilience scores related to each level are calculated using:

$$R_L = \frac{1}{3} \sum_L R_{L,S} \tag{6}$$

Moreover, the resilience scores related to each stage are calculated using the following expression:

$$R_S = \frac{1}{3} \sum_S R_{L,S} \tag{7}$$

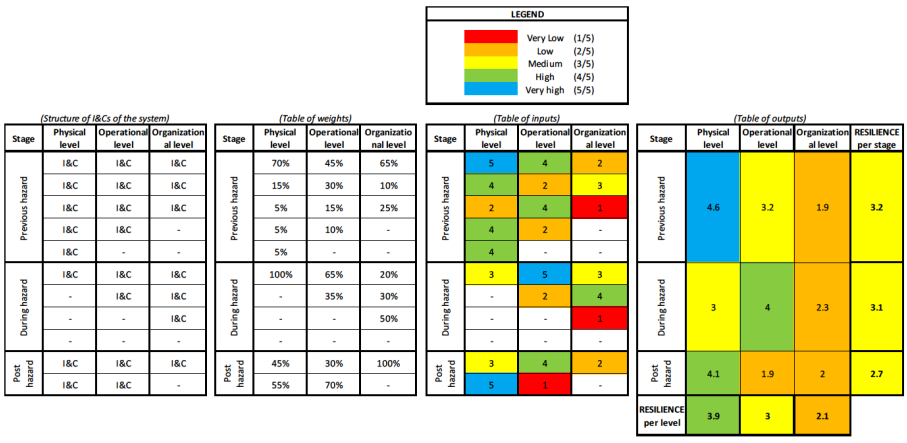

Figure 8. Description of the Quantitative Resilience Management Tool [44].

4.2.4. Resilience Capacities Metric

In [46], the authors introduced a metric for management systems as a solution for decision support and design. Similar to other quantification-based approaches, this proposed resilience metric aimed to link the three main resilience capacities (absorption, adaptation, and restoration) with recovery time. Their model [46], expressed in Figure 8, was employed

to evaluate a resilience factor ρ_i. Here, S_p represents the speed recovery factor value, F_o denotes the initial infrastructure performance level, F_r corresponds to the total performance after recovery, and F_d refers to the performance level immediately post-disruption.

$$\rho_i(S_p, F_r, F_d, F_o) = S_p \frac{F_r F_d}{F_o F_o}$$
$$where; S_p = \begin{cases} (t_\delta / t_r^*) exp[-a(t_r - t_r^*); for; t_r \geq t_r^*] \\ (t_\delta / t_r^*); otherwise \end{cases} \quad (8)$$

Furthermore, the authors discovered that these measures are generated based on the specific historical knowledge of each affected organization and also by applying the exact disruption event time, denoted by the indices t_δ—the slack time (maximum acceptable time post-disaster before recovery occurs) and t_r—the time to achieve the final recovery (attain equilibrium). In Equation (8), α describes the parameter measuring the "decay" in resilience, and t_r^* represents the time required to implement the recovery program and plan.

The time to recovery in this paper is assessed from the failure itself until the infrastructure restores an acceptable level of functionality. The model highlights the significance of the time to restart the infrastructure and taking the "slack time" into account. If the recovery process extends beyond the slack time, the resilience of the infrastructure will eventually decrease. Conversely, if the initial recovery is faster than the slack time, the resilience metric declines, and if the first recovery is considered effective but the infrastructure requires an extended period to recover after initial actions, the resilience metric also declines.

4.2.5. Multi-Dimensional Resilience Metric

In [47], the authors propose the model presented in Equation (9), which can be defined by measuring the rate of total potential damage over the time period T:

$$R(X, T) = \frac{T^* - XT/2}{T^*} = 1 - \frac{XT}{2T^*} \quad (9)$$

The components of this model used to determine the overall resilience in smart ICIs are described as follows: $X = (0; 1)$ represents the percentage of functionality lost after a disturbance, $T = (0; T)$ denotes the time required for complete recovery, and T signifies an extended period during which lost functionality is assessed. In the same study [47], the authors found that the equivalent level of resilience observed from the resilience triangle could be achieved by employing different combinations of X and T. Additionally, they present a visualization of the trade-offs between reduced functionality and recovery time for corresponding levels of resilience.

Limitations: While resilience based on the quantification approach is considered one of the most promising solutions for smart ICIs, the lack of data remains the most challenging aspect of conducting a resilience analysis using this measure. Companies are often unwilling to release data such as mean time to failure (MTTF) or mean time to repair (MTTR), and even when they do, the released data may not cover all actual events.

4.3. Dynamic System Approach

System dynamic simulation approaches have emerged as a solution for scientists to study infrastructure services, the consequences of disturbances, and the associated downstream results. Dynamic simulations also possess the capability to assess the impacts of policies and regulations on infrastructure processes. Numerous studies have developed specific dynamic simulations for various interdependent infrastructures, including energy infrastructures (electricity, oil, and natural gas), telecommunications systems, transportation systems (waterways, highways, and rail), emergency services, banking and finance infrastructure, agricultural sector, water systems, shipping systems, and market sectors [20]. In [48], the authors present a method for evaluating the resilience of smart ICIs based on designing operative dependencies and examining the operational responses to disruptions. They represent the infrastructure as a network model, where nodes and arcs between them

determine dependencies. This type of relationship is described as a network topology, represented by a dependency graph. A clear example of a dependency graph is shown in Figure 9.

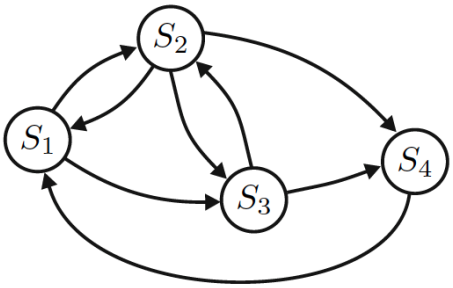

Figure 9. Interconnections of four systems [47].

In this method, each infrastructure is defined based on the functionality loss rate λ, recovery rate μ, and service threshold σ. The authors conduct a simple examination of two interconnected infrastructures, as illustrated in Figure 10. If $S1$ fails (i.e., its state threshold is exceeded), it ceases providing service to $S2$, which subsequently begins to fail. Two primary scenarios exist: (1) $S1$ recovers, meaning the state of $S1$ returns within its threshold σ_1, before $S2$ fails; (2) $S2$ fails before $S1$ recovers. In the latter case, both infrastructures become inoperative and incapable of regaining functionality, resulting in a deadlock wherein each system awaits the other's functional restoration. The components of the interconnected infrastructures are combined into a hypercube $[0,1]^n$. This collection can be divided into four disjoint subsets: the operation region O, the resilience region R, the non-resilience region $\bar{R}$, and the out-of-operation region $\bar{O}$. The following ratio provides an evaluation of the network resilience capacity:

$$c_r = \frac{M(R)}{M(R \cup \bar{R})} = \frac{M(R)}{M(R) + M(\bar{R}))} \in [0,1] \tag{10}$$

Studying the resilience of interconnected infrastructures is an original objective linked to other challenging goals, such as designing resilient controllers. In situations involving large-scale events, understanding response dynamics in the face of an incident is crucial. In complex, realistic obstacle environments, the recovery to standard functionality must be executed within prescribed time constraints, e.g., the maximum functional blackout a given infrastructure can tolerate.

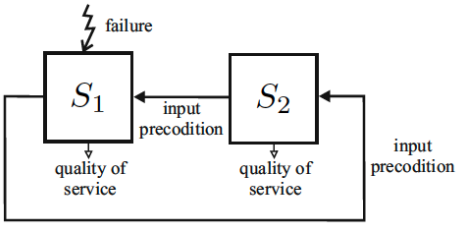

Figure 10. System composed of two subsystems with mutual functional dependency [47].

Limitations: This model faces limitations in its capacity to address all distinct stages and to incorporate every resilience capacity within each integrated model, as well as in overlapping with other concepts such as robustness, vulnerability, and fragility. Furthermore, scalability and accuracy also present significant challenges in this method.

4.4. Empirical Approach

The empirical approach is a prevalent method for evaluating resilience in smart Interdependent Critical Infrastructures (ICIs). This approach emphasizes data collection directly from the infrastructure to determine overall resilience, relying on historical reports

to assess the total resilience of the ICI. In [49], the authors propose an empirically based tool that examines ICI connectivity measurements derived from news, articles, and other reports on severe ICI impacts. Recently, databases dedicated to collecting empirical data have been established to monitor and report ICI events. However, these databases primarily focus on individual smart infrastructures rather than ICIs as a whole.

Many incidents, such as terrorist attacks on energy infrastructure, serve as examples of such databases. One notable example can be found in [49], a database containing public reports of ICI disruptions. Data in this database are gathered from open sources, including newspapers, articles, and news, and only high-impact events are recorded, e.g., those affecting at least 10,000 customers. Regularly occurring, limited, and planned operational disruptions are not included. Each event is characterized by various attributes, such as ICI sector and context, event start time, duration, affected geographical area, type of failure, losses and impact, recovery methods, and recommendations.

Another framework using a similar data type is presented in [50], where the authors develop an analytical structure with practical applications for understanding ICI failures. They utilize significant power outages as primary data to demonstrate how major problems in power infrastructure can cause issues in interconnected (interdependent) infrastructures. Their analysis is based on three real examples: the August 2003 northeastern North American blackout, the 1998 Quebec ice storm, and a series of three 2004 Florida hurricanes. Data were collected through news and internet reports, and measures were developed to efficiently identify possible outcomes based on the type of failures and affected regions. A comparison between all events is provided as a basis for considering the advantages of risk mitigation. In [51], a knowledge-based learning method for ICI is employed to acquire reports of common patterns of ICI failure following external disturbances. The knowledge-based discovery process combines ICI failure reports and demonstrates the procedure for transforming them into new data frames for data mining purposes. A data mining algorithm known as a generalized sequential pattern (GSP) is then applied to identify common patterns in ICI failure records. Figure 11 illustrates the five main steps of this approach, which helps clarify the most frequent failure events.

Figure 11. Knowledge discovery process for ICI [51].

Limitations: The collection of empirical data often focuses on specific failure types, such as cascading failures. However, there are numerous reasons why failures may propagate beyond CI sector boundaries and may not be captured in this type of data. Additionally, this data may lack accuracy since many failures are not reported in the news or at a technical level. Aside from the absence of accurate data, the database itself presents another limitation of the empirical approach, as no databases have been identified that concentrate on critical disturbances across all ICIs and cascading consequences using an "all-hazards" approach.

4.5. Economic Approach

In current research, economic resilience is defined as the "inherent ability and adaptive response that enables firms and regions to avoid maximum potential losses" [52]. The foundational model in [52] employs a linear time-independent analysis to examine various aspects that may influence overall resilience, such as generation, flow, and consumption of multiple products within ICIs. This model has also been extended to incorporate nonlinearities and time dependencies to investigate different hazard models within ICIs. Moreover, in [53], the authors characterize dependencies between infrastructures in simple terms, such as the exchange of products, data, and services. They also demonstrate how a disaster event can exacerbate initial damage based on these dependencies, resulting in

cascading failures. Consequently, understanding the dependencies within ICIs is a crucial aspect for decision makers to consider during the modeling and recovery processes. In their example, recovery is based on assessing infrastructure parameters from graph theory. This methodology was illustrated using a potential infrastructure system, including power, water, and telecommunication infrastructures following a hurricane.

Additionally, in [54], the authors present a risk-based economic input–output model, which serves as a useful tool for estimating the cascading effects of ICI failures. Their model is applied to provide a framework for evaluating economic resilience. They propose a static model for resilience that incorporates primary resilience concepts of robustness, rapidity, redundancy, and resourcefulness. The general notion of static resilience, or "the ability of infrastructure to maintain functionality during a disruptive event" [55], is depicted in Figure 12 and expressed in Equation (11):

$$Static\ Economic\ Resilience = \frac{\%\Delta DY^{max} - \%\Delta DY}{\%\Delta DY^{max}} \quad (11)$$

Here, $\%\Delta DY$ represents the actual percentage difference in infrastructure functionality following a disruptive event, and $\%\Delta DY^{max}$ denotes the maximum rate difference corresponding to the worst-case level of production.

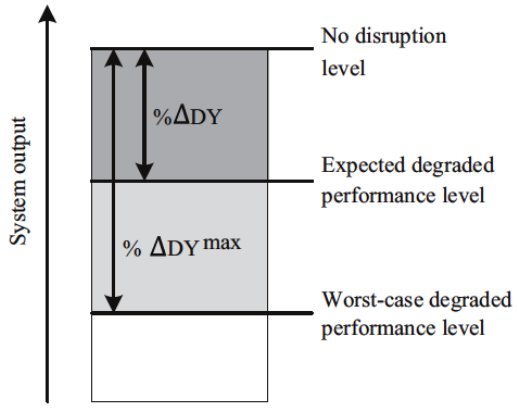

Figure 12. Static economic resilience quantification [54].

Limitations: The primary weaknesses of this approach are that many metrics related to this type are only for static resilience and focus on the disturbance event, which lacks the determination of resilience measures in pre/post-event phases, such as preparedness.

4.6. Network-Based Approach

The network-based approach seeks to understand data on dependencies by representing various components of the infrastructure as nodes within a network, where the presence of a connection between two nodes is depicted by a link connecting them. In paper [31], the authors present a resilience metric based on the infrastructure performance method during a period from 0 to T, which may involve multiple disruptive events, as illustrated in Figure 13. For a disruption event, time is divided into three phases: (1) a disaster prevention phase $(t_0 \leq t \leq t_1)$, (2) a loss propagation phase $(t_1 \leq t \leq t_2)$, and (3) an evaluation and recovery phase $(t_2 \leq t \leq t_3)$. These three phases can sequentially demonstrate the resistant, absorptive, and restorative capabilities of the infrastructure experiencing the disaster, and these capacities, shown from 0 to T, collectively define infrastructure resilience during that period. The overall resilience is then calculated based on the target performance curve $P_T(t)$ and the original performance curve $P_R(t)$:

$$R(T) = \int_0^T P_R(t)dt / \int_0^T P_T(t)dt \quad (12)$$

Note that various times T allow for different types of resilience: past resilience, present potential resilience, and anticipated potential resilience. This model primarily examines

the present potential resilience, where infrastructure components are constant through 0 to T and similar to those currently in place. For the case in which the present potential resilience $PT(t)$ is a fixed value 1.0 and when a risk has its existence governed by a Poisson process [56], the expected resilience $E[R(T)]$ is:

$$E[R(T)] = E\left[\frac{\int_0^T P_R(t)dt}{T}\right] = 1 - E\left[\frac{1}{T}\sum_{n=1}^{N(T)} IA_n(t_n)\right] = 1 - \lambda E[AI] \quad (13)$$

where $E[*]$ is the expected value; n is the event experience number; $N(T)$ is the total number of event experiences during T; t_n is the occurrence time of the nth event. Additionally, the random variable $IA_n(t_n)$ is defined as the space between the original performance curve and the target performance curve, called the impact area for the nth incident occurring at time t_n; $E(IA)$ is the expected impact area following the accidents considering all possible forces; and λ is the occurrence rate of the accidents per year.

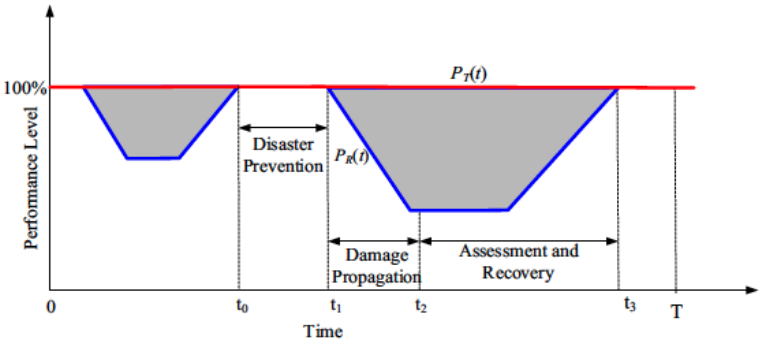

Figure 13. Typical performance process of an infrastructure during a time period T with multiple disruptive events [31].

In order to demonstrate a network-based framework for interdependent systems resilience assessment, the authors of [31] investigate the gas system in Harris County, Texas, USA. The gas compressors, gas storage facilities, gas delivery facilities, gas receipt facilities, and gas pipeline junctions are modeled as nodes, while the gas pipeline segments are described as links. The authors also investigate the effects resulting from the interdependencies among the systems by applying five different restoration strategies: random restoration, independent restoration, power first and gas second restoration, gas-aimed restoration, and power and gas compromised restoration.

Figure 14 displays the average restoration curves of the power and gas systems in Harris County, Texas, USA, under a hurricane scenario. This network-based approach is useful for understanding the complexities of interdependent infrastructure systems, helping decision makers plan and implement effective resilience strategies based on the unique characteristics and relationships between different infrastructure components. By considering various restoration strategies and analyzing their impacts on the performance of interdependent systems, this approach provides valuable insights into the most effective ways to enhance resilience in the face of disruptive events.

Limitations: While the network-based approach offers valuable insights for understanding interdependent infrastructure systems, it may not be suitable for all types of ICIs due to the specific topology of certain systems. For instance, the network-based metric might not be appropriate for telecommunication systems, as their static properties do not directly impact their ability to provide intended services (i.e., due to the presence of buffers, batteries, and multiple paths).

To address these limitations, researchers have suggested incorporating network dynamics into the analysis by superimposing flux dynamic models onto the topological structure. By considering both the static and dynamic properties of the network, this integrated approach can offer a more comprehensive understanding of the resilience of various ICIs, including those for which a purely network-based approach may not be sufficient.

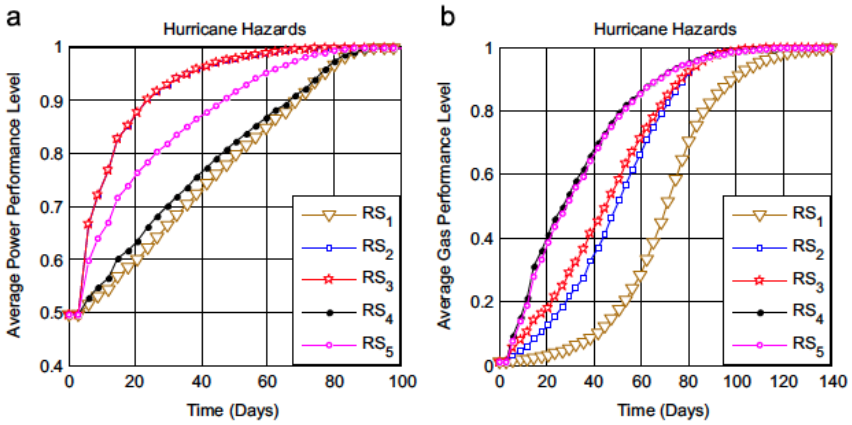

Figure 14. Average Restoration curves, where (**a**) shows the average power performance over disaster time, and (**b**) shows the average gas performance over disaster time in Harris County, Texas, USA [31].

4.7. Vulnerability Analysis Approach

The vulnerability analysis-based approach is a primary method for investigating and assessing the resilience of interdependent critical infrastructures (ICIs). In their study [57], the authors conducted a vulnerability analysis of ICIs, demonstrating the impact of dependencies on connected infrastructures. These effects can lead to significant economic disruptions and losses in various aspects. Their work examines two types of vulnerability: structural and functional vulnerability. A high-level overview of the vulnerability analysis process for ICIs is illustrated in Figure 15.

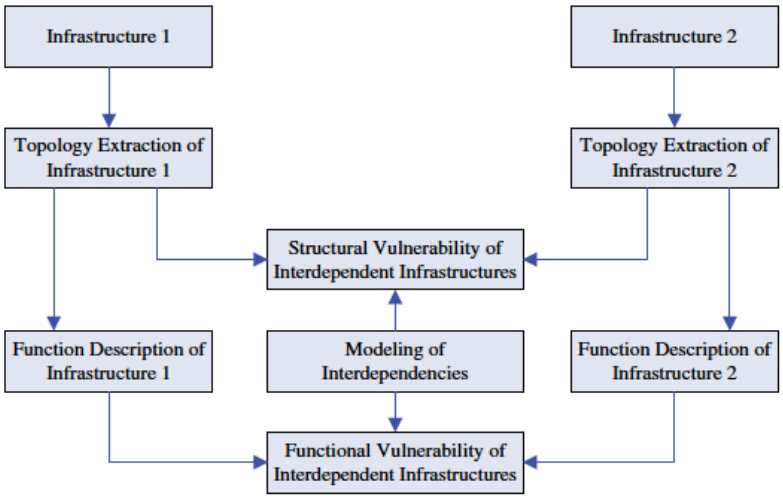

Figure 15. The vulnerability analysis process of interdependent infrastructures [57].

The topology is represented as a graph $G = (V, E)$, where $V = v_i$ is the set of vertices and E is the set of edges. The shortest path lengths connecting two nodes in the topology are denoted by $d(v_i, v_j)$. The structural efficiency $X(G)$ of infrastructure can then be defined as:

$$X(G) = \frac{1}{N_r N_I} \sum_{i \in G_T, j \in G_I} \frac{1}{d(v_i, v_j)} \tag{14}$$

Here, N_r represents the total number of support nodes, and N_I denotes the total number of load nodes. When two nodes are entirely unconnected or become disconnected due to attacks, their shortest path length $d(v_i, v_j)$ becomes infinite, and $1/d(v_i, v_j)$ equals zero. A high value for $X(G)$ indicates that the infrastructure is well-connected and has excellent performance. In the case of ICIs, the authors introduce a new parameter called

the interdependent effect. This parameter is defined as the absolute difference between the independent and interdependent efficiency, normalized by the maximum independent efficiency achieved at any extraction fraction:

$$\text{Independent}_{effect} = \frac{|\text{Interdependent Efficiency} - \text{Independent Efficiency}|}{max(\text{Independent Efficiency})} \quad (15)$$

For the independent scenario, the performance can be calculated for any given removal fraction. However, in the interdependent case, a fixed fraction of nodes will be removed from both infrastructures, and subsequently, the interdependent performance is evaluated for each network.

Limitations: The primary challenges of the vulnerability analysis-based approach are related to data availability and scalability, which can be further elaborated as follows:

Data Availability: Obtaining accurate and up-to-date data for interdependent critical infrastructures is often difficult due to security and privacy concerns. Additionally, proprietary information or sensitive data might not be publicly accessible, resulting in incomplete or outdated information for the analysis. This limitation can hinder the accurate assessment of the ICIs' resilience and vulnerability, leading to suboptimal decision making and risk management.

Scalability: The vulnerability analysis-based approach can become computationally expensive when applied to large-scale and complex ICIs, as it involves calculating the shortest path lengths and interdependent effects for numerous nodes and edges. As the size and complexity of the infrastructure networks increase, so does the required computational power and time. This challenge can make it difficult to efficiently analyze large-scale interdependent infrastructures and provide timely results for effective decision making and response planning.

These limitations highlight the need for alternative methods or improvements in data collection and computational efficiency to overcome the challenges associated with data availability and scalability in the vulnerability analysis-based approach for assessing the resilience of interdependent critical infrastructures.

4.8. Simulation-Based Approach

The simulation-based approach has recently gained traction as a useful method for decision makers to efficiently analyze the resilience of interdependent critical infrastructures (ICIs). In situations such as terrorist attacks on ICI systems, it is crucial to have simulation models that can accurately assess resilience and provide targeted solutions to address vulnerabilities in the infrastructure. A case study demonstrating the use of a simulation-based approach was presented by [58], which investigated the response capabilities of a fire department under various terrorist scenarios. The authors in [58] also proposed a discrete event simulation model, focusing on preparedness as a key factor in pre-event disruption resilience. Two types of simulation models were extensively discussed in their work: the first model deals with the social response or population dynamics following a terrorist attack, while the second model examines resource allocation management in affected areas. For both simulation models, resilience quantification was based on the response time (R_T). Additionally, in [59], the authors suggested employing a simulation-based approach within the supply chain context to assess resilience. Their simulation models were centered on three critical resilience factors: preparedness, responsiveness, and recovery, with the Introduction of Time Absolute Error (ITAE) as an innovative resilience measurement.

Limitations: One of the primary challenges in this approach is the complexity of modeling interdependent infrastructures to evaluate resilience. Moreover, an accurate simulation requires reliable data related to the infrastructure being modeled, which may not always be readily available. These limitations emphasize the need for better modeling techniques and data collection methods to enhance the effectiveness of the simulation-based approach for assessing the resilience of ICIs.

4.9. Seismic Resilience Approach

Seismic-related measures and approaches have been historically considered critical solutions for predicting the overall resilience of both standalone infrastructures and interdependent critical infrastructures (ICIs) [60]. A promising method has been introduced by the Multidisciplinary and National Center for Earthquake Engineering Research (MCEER).

MCEER developed a comprehensive resilience framework [37] to define the seismic resilience of infrastructure in response to a specific event, such as an earthquake. The impact of an earthquake can be estimated by calculating the predicted degradation in the quality of service associated with the infrastructure, $Q(t)$. Assuming an earthquake occurs at time t_0, this degradation is estimated for the period immediately following the shock (t_0) until $Q(t)$ recovers to its pre-earthquake levels (t_1). Resilience loss, RL, is determined as:

$$RL = \int_{t0}^{t1} [100 - Q(t)]dt \tag{16}$$

Alternatively, the overall system loss can be predicted based on the shaded area in Figure 16. The framework assumes that infrastructure performance levels are at 100 percent before the shock event and will recover to this level after the earthquake. Although this approach is demonstrated in the context of earthquakes, it can be adapted for other types of shocks as well.

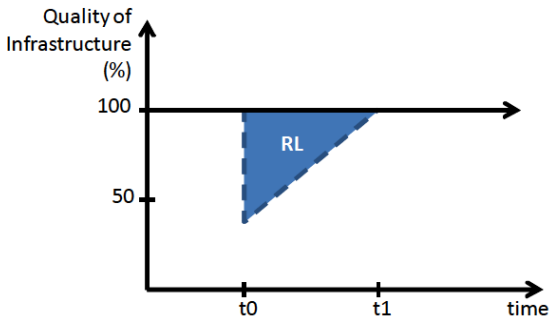

Figure 16. Conceptual illustration of MCEER's seismic resilience loss measurement [37].

Limitations: As one of the oldest approaches for measuring ICIs resilience, the seismic approach has several weaknesses. One significant limitation is its time-dependent (static) nature, which only considers the event time and does not cover all resilience phases (i.e., anticipation, absorption, and adaptation) along the timeline. Furthermore, this approach relies heavily on accurate and available data, which may not always be feasible.

4.10. Probability-Based Resilience Approach

The probability-based resilience estimation is a traditional method that has been used historically to help infrastructures predict event occurrences based on historical data. In [61], the authors introduced a probabilistic method for estimating the total infrastructure resilience. They mathematically described it in Equation (17) concerning predefined performance standards A, given a seismic event of size i:

$$R = P(A|i) = P(r_0 < r^* and; t_1 < t^*) \tag{17}$$

where r_0 = initial infrastructure function loss; r^* = a determined standard of robustness representing the "highest tolerable loss" in infrastructure function after a disturbance event; t_1 = time to complete recovery; and t^* = the "highest tolerable disruption time", i.e., the maximum acceptable duration for infrastructure function to return to pre-earthquake levels. They defined resilience R as "the probability that the system of interest will meet predefined performance standards in a seismic event of magnitude i" (Equation (17)). Figure 17 illustrates the use of each element and how they are estimated. The authors focused on assessing resilience concerning the changes in the infrastructure function product.

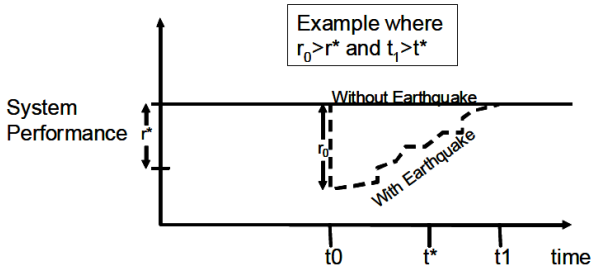

Figure 17. Measuring probabilistic resilience [61].

Limitations: The probability-based approach heavily relies on data to estimate the likelihood of an event occurring and its potential impact on infrastructure resilience. However, the availability and reliability of such data pose significant challenges. For instance, the historical data used for probability calculations may not accurately represent the current state of the infrastructure or the potential risks it faces. Additionally, the data may not be complete or may be biased towards certain types of events, leading to inaccurate predictions. Therefore, it is crucial to ensure that the data used in probability-based approaches are up-to-date, accurate, and comprehensive to obtain reliable estimates of infrastructure resilience.

This paper presents a summary of all the methods and metrics used for determining the resilience of Smart ICIs, as shown in Table 3. The classification used in this table is based on the modeling strategies presented in [20], with the addition of four approaches: indicator-based, quantification-based, seismic-based, and probability-based approaches. The table indicates the model and threat type associated with each method. For instance, the LIOH approach in the indicator-based method uses the level-based model to detect resilience and can be applied to all types of threats.

Table 3. Resilience Measures for Smart Critical Infrastructure in the Literature.

Resilience Approach	Metric	Model	Threat Type
Indicator-based approach	ANL [36]	Level-based	All-hazards
	LIOH [38]	Level-based	All-hazards
	REWI [38]	Level-based	All-hazards
	SmartResilience [39]	Level-based	All-hazards
	DHS-IST [40]	Level-based	All-hazards
	AHA [41]	Level-based	All-hazards
Quantitative (holistic) approach	MOP-GR [42]	Time-based	All-hazards
	FLEP [43]	Time-based	All-hazards
	QRMP [44]	Indicator-based	All-hazards
	RCM [46]	Time-based	All-hazards
	MDRM [47]	Time-based	All-hazards
Dynamic system approach	C_r [48]	Functional-dependent	Cyber
Empirical approach	Event metrics [49]	Data-based	Cascading
	IFI [50]	Data-based	All-hazards
	GSP [51]	Knowledge-based	System failures
Economic approach	Operability [53]	Graph-based	All-hazards
	SER [54]	Static-based	All-hazards
Network-based approach	R(T) [31]	Time-based	Hurricane
Vulnerability analysis approach	ieffect [57]	Network-based	Cyber
Simulation-based approach	R_T [58]	Time-based	Terror-attack
Seismic resilience approach	RL [37]	Time-based	earthquakes
Probability-based approach	Prob_R [61]	Probability-based	earthquakes

The approaches are categorized based on the method used to quantify resilience and the type of data used, such as historical data, news data, and data based on previous events. While all methods can be used, some methods are more preferred than others depending on the situation, such as the availability of accurate and reliable data. For example, if the available information is based on news and reports, such as the number of available power lines during a disruption event, then empirical models are preferred. On the other hand, if the interdependent infrastructures can be modeled as a graph, and accurate data are available, then the network-based approach is more preferred in such a situation.

5. Resilience Assessment for Smart Power and Telecommunication: Case Study

The electric power network is considered one of the most crucial infrastructures in the event of a hazardous occurrence. Scientists have identified failure types of electric power infrastructure and the consequences of power outages following natural or human-made disasters [62]. The core critical facilities of the electric power infrastructure include generation power plants, transmission substations, and transmission and distribution lines. Transmission lines connect generation power plants to transmission substations, which deliver high-voltage electricity over long distances. If any of these plants or materials are physically damaged or if supporting infrastructures such as operation systems collapse, the electric power infrastructure may experience severe effects and potentially a complete failure [63].

In addition to the power grid, telecommunication infrastructure is also considered one of the leading critical infrastructures in smart cities, providing a pathway for data transmission. The fundamental connections can be classified into three different levels: landlines, airwaves, and satellite links [64]. Both systems are interdependent on each other, and various resilience approaches have been proposed to overcome the failure event in any of the systems that develop after a disaster occurs [65,66].

In this section, we present a case study that demonstrates essential measures for assessing the resilience of interdependent electrical and communication grids. The case study examines the feasibility and applicability of the General Resilience (GR) quantitative method for the Swiss electric power supply system (EPSS), which is considered an exemplary application. The study conducted by Nan et al. [67] utilizes a hybrid modeling simulation approach to represent the behavior and functionalities of each subsystem, as shown in Figure 18. The EPSS is viewed as three interrelated subsystems, including the system under control (SUC), the operational control system (OCS), and the social system (SS). SUC and OCS are regarded as technical systems, while SS is viewed as non-technical.

The resilience capabilities, including the absorptive, adaptive, and restorative capability, are identified and integrated into a unique resilience metric, which combines these capabilities into a comprehensive view of the system's resilience in different phases. The metric proposed is the General Resilience (GR), which integrates measures of robustness (R), rapidity (RAPI), performance loss (PL), the time-averaged performance loss (TAPL), and recovery ability (RA) into a simultaneous quantification. This metric is unique in its complete dependence on time and ability to merge all three required capabilities.

The case study deploys a two-layer Agent-Based Simulation Modeling approach to integrate time-dependent stochastic factors into the vulnerability assessment of the electric power system. The simulation is based on the assumption that a natural hazard, such as a winter storm, impacts the central zone of Switzerland, where power transmission lines are located, resulting in the disconnection of 17 transmission lines out of 219 lines. The analysis is a causal data analysis that investigates what happens to one variable when another variable changes.

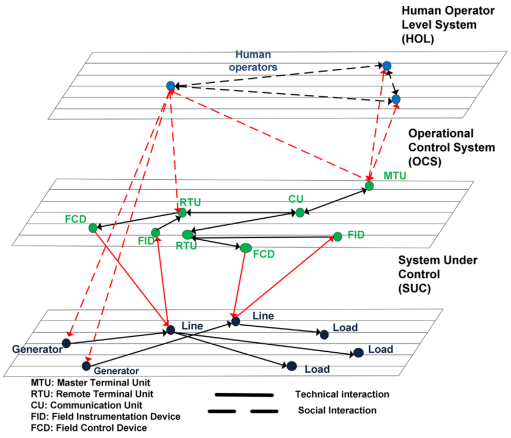

Figure 18. The representation of the EPSS in three subsystems (layers).

Overall, this case study demonstrates how the GR method (3) can be utilized to estimate the interdependent resilience index of the EPSS. The proposed method and metric provide a holistic view of the system's resilience and allow for comparisons across multiple systems and configurations. The study highlights the importance of considering interdependent infrastructures and the need for a comprehensive approach to resilience assessment.

The Swiss high-voltage electric power supply system (EPSS) is illustrated in Figure 19, which consists of 219 transmission lines and 129 substations.

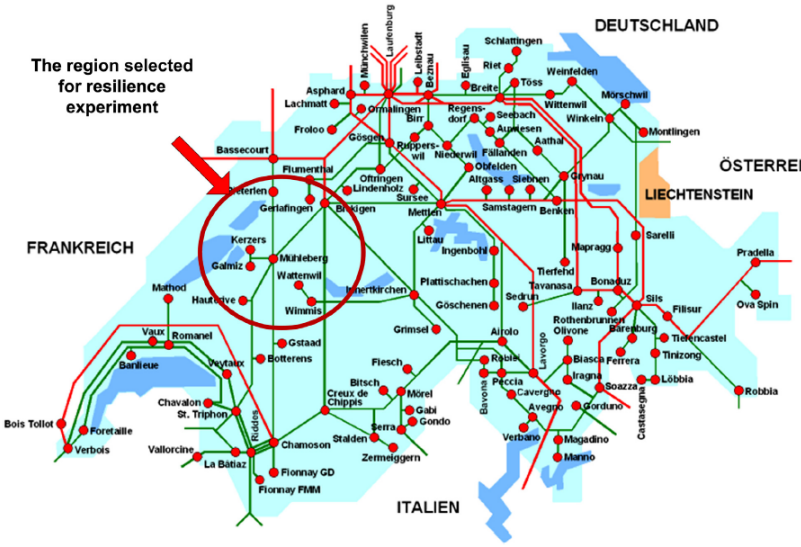

Figure 19. The high voltage Swiss electric power transmission system.

In this case study, the performance of the scrutinized system is evaluated using two distinct measurements, each addressing unique aspects of the infrastructure's characteristics. The first measurement centers around the total quantity of available transmission lines, a parameter that directly reflects the system's topology. The second measurement, on the other hand, assesses the precise amount of power demand that the system can cater to, offering insights into its functional capabilities.

To further investigate the performance, a multi-objective optimization problem (MOP) is defined for the Supervisory Control and Data Acquisition (SCADA) system, an integral part of the infrastructure. This selected MOP is intrinsically tied to the system's topology, focusing specifically on the total number of Remote Terminal Units (RTUs) at its disposal.

It is vital to recognize that the selection of a suitable MOP for the SCADA system is influenced by various factors, including the overarching goals of the system, the resources at its disposal, and the system's specific constraints. Consequently, the selected

MOP should be in harmony with the performance metrics employed for evaluating the system's effectiveness.

To facilitate comparisons, the MOPs are normalized within the range of [0, 1]. This normalization process helps in keeping the diverse measurements within a standard scale, enabling a more accurate and fair comparison. In the broader setting, the case study provides a comprehensive analytical framework that captures key elements of system resilience while addressing the inherent complexities and interdependencies within the infrastructure.

$$MOP_{SUC1} = \frac{\text{number of available transmission lines}}{\text{number of total transmission lines}} \in [0,1] \tag{18}$$

$$MOP_{SUC2} = \frac{\text{actual power demand served (MW)}}{\text{total power demand (MW)}} \in [0,1] \tag{19}$$

$$MOP_{SCADA1} = \frac{\text{number of available RTU devices}}{\text{number of total RTU devices}} \in [0,1] \tag{20}$$

To conduct a thorough and effective assessment of the resilience metric, General Resilience (GR), vis-à-vis alternative strategies, it is imperative to calculate a couple of additional performability metrics. These metrics provide complementary perspectives on system performance and enhance our understanding of the system's resilience.

The first metric is the Average Substation Service Availability Index (ASSAI). This index quantifies the proportion of the total hours during which all operational substations render service in relation to the total hours wherein the service is demanded. This index offers a comprehensive view of the service available throughout the entire system, taking into account the operational status of all substations.

By comparing the ASSAI values of various solutions, one can gain a deeper understanding of their capacity to provide a dependable service over an extended period. This comparison provides an analytical perspective that is invaluable in understanding the system's resilience and effectiveness. Notably, the ASSAI serves as an essential tool for evaluating the dependability and robustness of the system's service, hence playing a pivotal role in the overall resilience assessment.

These combined metrics—GR and ASSAI—allow for a more holistic and nuanced understanding of system resilience. By integrating various aspects of system performance, they provide a comprehensive picture of system resilience, thereby facilitating informed decision making in the design and operation of resilient infrastructures.

$$\text{ASSAI} = \frac{N_S \times \text{number of hours} - \sum_{i=1}^{N_S} Res_i}{N_S \times \text{number of hours}} \in [0,1] \tag{21}$$

where Res_i represents the restoration time for the $i-th$ substation if service interruption exists and N_S represents the total number of substations. They experiment with the two systems under deploying different strategies, two strategies for the SUC system and one for SCADA systems; after applying each strategy in each system, they measure the resilience *GR* value, disruptive phase capabilities (*Robustness (R)*,*rapidity (RAPI)*, *performance loss (PL)*), and Recovery Phase capabilities(*rapidity (RAPI)*, *performance loss (PL)*) of each system under different experiments design (Mean Time To Repair (MTTR), Human error probability (HEP)). After that, they compare results from SUC and SCADA systems using coefficient correlation to understand the interdependence effects on each other shown in Figure 20. The directed impact of physical interdependence between SUC and SCADA are viewed in the left side of the figure. Higher numbers conclude that actions affecting the functionality, e.g., performance loss of the system, will directly result in an impact on the corresponding functionality of the other system that is dependent upon it. Hence, the impacts of improving the resilience of a system can result in a much more critical effect on an interdependent system.

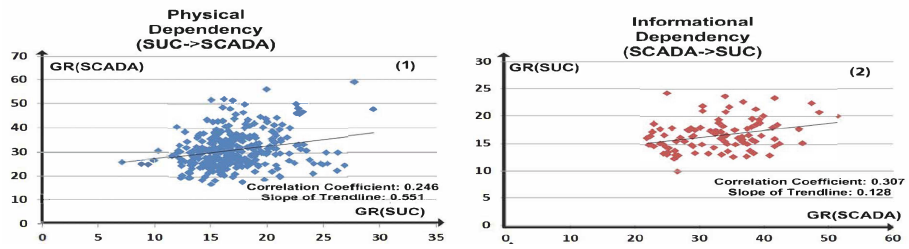

Figure 20. The average system performance under different experiments, where (1) shows the physical dependency and (2) shows the informational dependency

6. Conclusions

This paper examines an array of resilience models and measurements that have been meticulously designed for interconnected, essential smart infrastructures, also known as Smart ICIs. It encompasses a vast array of associated terminology and definitions, delves deeply into universally acknowledged stages and capacities of resilience, and investigates in depth a variety of potential failure types that could disrupt Smart ICIs.

In addition, the paper elucidates each metric in great detail and provides a comprehensive comprehension of the employed methods, illustrated with case studies. In addition, it introduces a variety of resilience strategies tailored to various resilience phases, articulating these strategies in a manner that is simple to comprehend.

As the paper nears its conclusion, it focuses on a quantification-based approach, supplemented by a pertinent case study, that exemplifies the practical application of interdependent resilience metrics in tangible, real-world situations. In addition, there is a concise summary of the most common obstacles encountered when assessing Smart ICI resilience metrics. Given the rapidly expanding understanding of Smart ICIs, it is imperative that all stakeholders confront these challenges head-on and endeavor to develop even more precise and effective resilience metrics and models.

This exhaustive review serves as an invaluable resource for policymakers, researchers, and industry professionals committed to enhancing the resilience of interdependent smart critical infrastructures. With a comprehensive grasp of the various metrics and models, as well as an understanding of the complexities involved in assessing resilience, stakeholders are better able to make informed decisions and implement more effective strategies to protect these vital systems. In a world that is becoming increasingly interconnected, the ongoing evolution and improvement of resilience metrics and models will be crucial for ensuring the safety, security, and sustainability of smart interdependent critical infrastructures.

Despite the scope and depth of this study, certain limitations must be acknowledged. It is difficult to develop universally applicable tools due to the fact that resilience metrics and models are highly dependent on the context, the characteristics of the specific infrastructure, and the nature of potential threats. In addition, the current study focuses predominantly on theoretical aspects and case studies, which, despite providing invaluable insights, may not fully reflect the variety of real-world scenarios and operational constraints that can significantly impact the resilience of Smart ICIs.

There are numerous opportunities for further research and development in this field moving forward. Future research may investigate the development and implementation of dynamic resilience models that can adapt to changing conditions and evolving threats. Additionally, it may be advantageous to investigate the integration of machine learning and artificial intelligence techniques to improve the predictive capabilities of these models, thereby allowing for more proactive resilience-building measures. Future research could also concentrate on the implementation of these models and metrics, as well as the creation of decision-support tools for policymakers and industry professionals. To increase the resilience of Smart ICIs, these instruments could facilitate more effective planning, investment, and operational decisions. In a world that is becoming increasingly complex and interconnected, these future endeavors will play a vital role in advancing our understanding and administration of resilience.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large group Research Project under grant number RGP.2/550/44.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rezvani, S.M.; Falcão, M.J.; Komljenovic, D.; de Almeida, N.M. A Systematic Literature Review on Urban Resilience Enabled with Asset and Disaster Risk Management Approaches and GIS-Based Decision Support Tools. *Appl. Sci.* **2023**, *13*, 2223. [CrossRef]
2. The World Bank. World Bank Open Data. 2023. Available online: https://data.worldbank.org/ (accessed on 1 April 2023).
3. McLaren, D.; Agyeman, J. *Sharing Cities: A Case for Truly Smart and Sustainable Cities*; MIT Press: Cambridge, MA, USA, 2015.
4. The Royal Academy of Engineering. *Smart Infrastructure: The Future*; The Royal Academy of Engineering: London, UK, 2012.
5. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consum. Electron. Mag.* **2016**, *5*, 60–70. [CrossRef]
6. Chen, M.; Jiang, Y.; Wang, E.; Wang, Y.; Zhang, J. Measuring Urban Infrastructure Resilience via Pressure-State-Response Framework in Four Chinese Municipalities. *Appl. Sci.* **2022**, *12*, 2819. [CrossRef]
7. Arroub, A.; Zahi, B.; Sabir, E.; Sadik, M. A literature review on Smart Cities: Paradigms, opportunities and open problems. In Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 26–29 October 2016; pp. 180–186.
8. Tubaishat, M.; Qi, Q.; Shang, Y.; Shi, H. Wireless Sensor-Based Traffic Light Control. In Proceedings of the 2008 5th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA , 10–12 January 2008; pp. 702–706. [CrossRef]
9. Hurst, W.; Bennin, K.E.; Kotze, B.; Mangara, T. Critical Infrastructures: Reliability, Resilience and Wastage. *Infrastructures* **2022**, *7*, 37. [CrossRef]
10. Imteaj, A.; Khan, I.; Khazaei, J.; Amini, M.H. Fedresilience: A federated learning application to improve resilience of resource-constrained critical infrastructures. *Electronics* **2021**, *10*, 1917. [CrossRef]
11. Rifaid, R.; Abdurrahman, A.; Baharuddin, T.; Kusuma, B.M.A. Smart City Development in the New Capital City: Indonesian Government Plans. *J. Contemp. Gov. Public Policy* **2023**, *4*, 115–130. [CrossRef]
12. Zakariya, M.; Teh, J. A Systematic Review on Cascading Failures Models in Renewable Power Systems with Dynamics Perspective and Protections Modeling. *Electr. Power Syst. Res.* **2023**, *214*, 108928. [CrossRef]
13. de Oliveira, A.K.B.; Battemarco, B.P.; Barbaro, G.; Gomes, M.V.R.; Cabral, F.M.; de Oliveira Pereira Bezerra, R.; de Araújo Rutigliani, V.; Lourenço, I.B.; Machado, R.K.; Rezende, O.M.; et al. Evaluating the Role of Urban Drainage Flaws in Triggering Cascading Effects on Critical Infrastructure, Affecting Urban Resilience. *Infrastructures* **2022**, *7*, 153. [CrossRef]
14. Villar Miguelez, C.; Monzon Baeza, V.; Parada, R.; Monzo, C. Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. *Smart Cities* **2023**, *6*, 728–743. [CrossRef]
15. Clinton, W. *Presidential Decision Directive 63*; The White House: Washington, DC, USA, 1998. Available online: fas.org/irp/offdocs/pdd/pdd-63.htm (accessed on 27 April 2023).
16. National Infrastructure Advisory Council (US); Noonan, T.; Archuleta, E. *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*; DHS/NIAC: Washington, DC, USA, 2009.
17. Bush, G.W. The national strategy for the physical protection of critical infrastructures and key assets. In *Technical Report*; Executive Office of the President: Washington, DC, USA, 2003.
18. Bush, G.W. The national security strategy of the United States of America. In *Technical Report*; Executive Office of the President: Washington, DC, USA, 2002.
19. Roche, E.M. Critical Foundations: Protecting America's Infrastructures, 1998. Available online: https://www.google.com.hk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiv-M6Rp4r_AhUL3WEKHVzNAXIQFnoECAwQAQ&url=https%3A%2F%2Fsgp.fas.org%2Flibrary%2Fpccip.pdf&usg=AOvVaw1xHbuRO7HxLgmkiun55WO5 (accessed on 1 January 2023).
20. Rinaldi, S. Modeling and simulating critical infrastructures and their interdependencies. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004; p. 8. [CrossRef]
21. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **2001**, *21*, 11–25. [CrossRef]
22. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 43–60. [CrossRef]
23. Halkos, G.E.; Gkampoura, E.C. Reviewing usage, potentials, and limitations of renewable energy sources. *Energies* **2020**, *13*, 2906. [CrossRef]
24. Almaleh, A.; Tipper, D.; Al-Gahtani, S.F.; El-Sehiemy, R. A Novel Model for Enhancing the Resilience of Smart MicroGrids' Critical Infrastructures with Multi-Criteria Decision Techniques. *Appl. Sci.* **2022**, *12*, 9756. [CrossRef]

25. Parandehgheibi, M.; Modiano, E.; Hay, D. Mitigating cascading failures in interdependent power grids and communication networks. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014, Venice, Italy, 3–6 November 2014; pp. 242–247. [CrossRef]
26. Woods, D.D. Four concepts for resilience and the implications for the future of resilience engineering. *Reliab. Eng. Syst. Saf.* **2015**, *141*, 5–9. [CrossRef]
27. Longstaff, P.H.; Armstrong, N.J.; Perrin, K.; Parker, W.M.; Hidek, M.A. Building resilient communities: A preliminary framework for assessment. *Homel. Secur. Aff.* **2010**, *6*, 1–23.
28. House, W. *Empowering Local Partners to Prevent Violent Extremism in the United States*; The White House: Washington, DC, USA, 2011.
29. Cohen, D.K.; Cuéllar, M.-F.; Weingast, B.R. Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates. *Stanf. Law Rev.* **2006**, *59*, 673–759. Available online: http://www.jstor.org/stable/40040307 (accessed on 24 February 2023).
30. Institution of Civil Engineers (ICE). Seismic Performance Assessment of Buildings. In *Methodology*; FEMA P-58; Federal Emergency Management Agency: Washington, DC, USA, 2018; Volume 1.
31. Ouyang, M.; Wang, Z. Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliab. Eng. Syst. Saf.* **2015**, *141*, 74–82. [CrossRef]
32. Walther, G.; Jovanovic, M.; Vollmer, M.; Desmond, G.; Choudhary, A.; Auerkari, P.; Tuurna, S.; Pohja, R.; Koivisto, R.; Molarius, R.; et al. *Report on Challenges for SCIs*; IVL Swedish Environmental Research Institute: Östersund, Sweden, 2016.
33. Norris, F.H.; Stevens, S.P.; Pfefferbaum, B.; Wyche, K.F.; Pfefferbaum, R.L. Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *Am. J. Community Psychol.* **2008**, *41*, 127–150. [CrossRef]
34. Almaleh, A.; Tipper, D. Risk-Based Criticality Assessment for Smart Critical Infrastructures. *Infrastructures* **2022**, *7*, 3. [CrossRef]
35. Patel, S.S.; Rogers, M.B.; Amlôt, R.; Rubin, G.J. What do we mean by 'community resilience'? A systematic literature review of how it is defined in the literature. *PLoS ONE* **2017**, *12*, e0170100.
36. Fisher, R.; Bassett, G.; Buehring, W.; Collins, M.; Dickinson, D.; Eaton, L.; Haffenden, R.; Hussar, N.; Klett, M.; Lawlor, M.; et al. *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program*; Technical Report; Decision and Information Sciences; Argonne National Lab. (ANL): Argonne, IL, USA, 2010.
37. Bruneau, M.; Chang, S.E.; Eguchi, R.T.; Lee, G.C.; O'Rourke, T.D.; Reinhorn, A.M.; Shinozuka, M.; Tierney, K.; Wallace, W.A.; Von Winterfeldt, D. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthq. Spectra* **2003**, *19*, 733. [CrossRef]
38. Øien, K.; Massaiu, S.; Tinmannsvik, R.K.; Størseth, F. Development of early warning indicators based on Resilience Engineering. In Proceedings of the 10th International Conference on Probabilistic Safety Assessment and Management 2010, PSAM 2010, Seattle, WA, USA, 7–11 June 2010; Volume 3, pp. 1762–1771.
39. Jovanovi, A.; Ø, K.; Choudhary, A. An Indicator-Based Approach to Assessing Resilience of Smart Critical Infrastructures. In *Urban Disaster Resilience and Security*; Springer: Cham, Switzerland, 2018; pp. 285–311.
40. Seidelsohn, K.; Voss, M.; Krüger, D. *Urban Disaster Resilience and Security*; Springer: Cham, Switzerland, 2018; p. 513. [CrossRef]
41. Fisher, R.; Norman, M.; Peerenboom, J. Resilience History and Focus in the USA. In *Urban Disaster Resilience and Security: Addressing Risks in Societies*; Springer: Cham, Switzerland, 2018; pp. 91–109. [CrossRef]
42. Nan, C.; Sansavini, G.; Kröger, W.; Heinimann, H. A quantitative method for assessing the resilience of infrastructure systems. In Proceedings of the PSAM 2014—Probabilistic Safety Assessment and Management, Honolulu, Hawaii, 14–18 June 2014.
43. Panteli, M.; Mancarella, P.; Trakas, D.N.; Kyriakides, E.; Hatziargyriou, N.D. Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems. *IEEE Trans. Power Syst.* **2017**, *32*, 4732–4742. . [CrossRef]
44. for Critical INfraStructure, R.E.R. Qualitative, Semi-Quantitative and Quantitative Methods and Measures for Resilience Assessment and Enhancement. *Procedia Comput. Sci.* **2016**, *176*, 2625–2634.
45. *Realising European ReSILiencE for Critical INfraStructure*; RESILENS timeline; RESILENS: Palo Alto, CA, USA, 2016.
46. Francis, R.; Bekera, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 90–103.. [CrossRef]
47. Zobel, C.W. Representing perceived tradeoffs in defining disaster resilience. *Decis. Support Syst.* **2011**, *50*, 394–403. [CrossRef]
48. Alessandri, A.; Filippini, R. Evaluation of Resilience of Interconnected Systems Based on Stability Analysis. *Lect. Notes Comput. Sci.* **2013**, *7722* , 180–190. [CrossRef]
49. Luiijf, E.; Nieuwenhuijs, A.; Klaver, M.; van Eeten, M.; Cruz, E. Empirical Findings on Critical Infrastructure Dependencies in Europe. In Proceedings of the Critical Information Infrastructure Security, Rome, Italy, 13–15 October 2008 ; Setola, R., Geretshuber, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 302–310.
50. McDaniels, T.; Chang, S.; Peterson, K.; Mikawoz, J.; Reed, D. Empirical Framework for Characterizing Infrastructure Failure Interdependencies. *J. Infrastruct. Syst.* **2007**, *13*, 175–184. [CrossRef]
51. Chou, C.C.; Tseng, S.M. Collection and Analysis of Critical Infrastructure Interdependency Relationships. *J. Comput. Civ. Eng.* **2010**, *24*, 539–547. [CrossRef]
52. Haimes, Y.Y.; Jiang, P. Leontief-Based Model of Risk in Complex Interconnected Infrastructures. *J. Infrastruct. Syst.* **2001**, *7*, 1–12. [CrossRef]
53. He, X.; Cha, E.J. Modeling the damage and recovery of interdependent critical infrastructure systems from natural hazards. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 162–175. [CrossRef]

54. Pant, R.; Barker, K.; Zobel, C.W. Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors . *Reliab. Eng. Syst. Saf.* **2014**, *125*, 92–102. [CrossRef]
55. Rose, A. Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environ. Hazards* **2007**, *7*, 383–398. [CrossRef]
56. Ouyang, M.; Dueñas-Osorio, L.; Min, X. A three-stage resilience analysis framework for urban infrastructure systems. *Struct. Saf.* **2012**, *36–37*, 23–31. [CrossRef]
57. Ouyang, M.; Hong, L.; Mao, Z.J.; Yu, M.H.; Qi, F. A methodological approach to analyze vulnerability of interdependent infrastructures. *Simul. Model. Pract. Theory* **2009**, *17*, 817–828. [CrossRef]
58. Albores, P.; Shaw, D. Government preparedness: Using simulation to prepare for a terrorist attack. *Comput. Oper. Res.* **2008**, *35*, 1924–1943. [CrossRef]
59. Spiegler, V.L.M.; Naim, M.M.; Wikner, J. A control engineering approach to the assessment of supply chain resilience. *Int. J. Prod. Res.* **2012**, *50*, 6162–6187. [CrossRef]
60. Cao, X.Y.; Feng, D.C.; Beer, M. Consistent seismic hazard and fragility analysis considering combined capacity-demand uncertainties via probability density evolution method. *Struct. Saf.* **2023**, *103*, 102330. . [CrossRef]
61. Chang, S.E.; Shinozuka, M. Measuring improvements in the disaster resilience of communities. *Earthq. Spectra* **2004**, *20*, 739–755. [CrossRef]
62. Winkler, J.; Dueñas-Osorio, L.; Stein, R.; Subramanian, D. Performance assessment of topologically diverse power systems subjected to hurricane events. *Reliab. Eng. Syst. Saf.* **2010**, *95*, 323–336. [CrossRef]
63. Mimura, N.; Yasuhara, K.; Kawagoe, S.; Yokoki, H.; Kazama, S. Damage from the Great East Japan Earthquake and Tsunami—A quick report. *Mitig. Adapt. Strateg. Glob. Chang.* **2011**, *16*, 803–818. [CrossRef]
64. Garshnek, V.; Barkle, J. Telecommunications systems in support of disaster medicine: Applications of basic information pathways. *Ann. Emerg. Med.* **1999**, *34*, 213–218. [CrossRef] [PubMed]
65. Miranda, K.; Molinaro, A.; Razafindralambo, T. A survey on rapidly deployable solutions for post-disaster networks. *IEEE Commun. Mag.* **2016**, *54*, 117–123. [CrossRef]
66. Gomes, T.; Tapolcai, J.; Esposito, C.; Hutchison, D.; Kuipers, F.; Rak, J.; De Sousa, A.; Iossifides, A.; Travanca, R.; Andre, J.; et al. A survey of strategies for communication networks to protect against large-scale natural disasters. In Proceedings of the 2016 8th International Workshop on Resilient Networks Design and Modeling, RNDM 2016, Halmstad, Sweden, 13–15 September 2016; pp. 11–22. [CrossRef]
67. Nan, C.; Sansavini, G.; Kröger, W. Building an integrated metric for quantifying the resilience of interdependent infrastructure systems. In *Critical Information Infrastructures Security: 9th International Conference, CRITIS 2014, Limassol, Cyprus, 13–15 October 2014*; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer International Publishing: Cham, Switzerland, 2016; Volume 8985, pp. 159–171. [CrossRef]