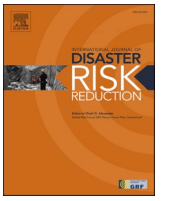
International Journal of Disaster Risk Reduction 124 (2025) 105535

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

journal homepage: www.elsevier.com/locate/ijdrr



Threat-agnostic resilience: Framing and applications

Benjamin D. Trump [a], Stergios-Aristoteles Mitoulis [b,*], Sotirios Argyroudis [c], Gregory Kiker [d], José Palma-Oliveira [e], Robert Horton [d,f], Gianluca Pescaroli [g], Elizaveta Pinigina [h], Joshua Trump [i], Igor Linkov [d,j]

[a] *Resilience Analytics, United States*
[b] *University of Birmingham, United Kingdom*
[c] *Brunel University of London, United Kingdom*
[d] *University of Florida, United States*
[e] *University of Lisbon, Portugal*
[f] *Dallas-Fort Worth International Airport, United States*
[g] *University College London, United Kingdom*
[h] *London School of Economics, United Kingdom*
[i] *Virginia Tech, United States*
[j] *Carnegie Mellon University, United States*

A R T I C L E I N F O

Keywords:
Resilience
Threat agnostic
Compounding threats
Sustainability
Critical infrastructure
Environment

A B S T R A C T

Critical infrastructure is not indestructible. Interdependencies between infrastructure systems and the environment compound consequences at vulnerable locations but can be harnessed to maximize operational efficiency, recovery capability, and long-term sustainability. Threats, both emergent and systemic, have propagated beyond historical norms, exposing the limitations of hazard-specific resilience approaches. These approaches, by their nature, rely on predefined scenarios that fail to capture the full complexity of cascading failures, novel threat combinations, and the dynamic evolution of risks over time, especially in the cases where environment is affected. This leaves critical gaps in planning, response, and recovery, as systems designed around specific hazards are often unable to adapt to disruptions that fall outside their narrowly defined parameters, resulting in unanticipated vulnerabilities and slower recovery trajectories. We propose a paradigm shift toward threat-agnostic resilience, emphasizing adaptability to unforeseen hazards through modularity, distributedness, diversity, and plasticity. These principles foster system-wide robustness by enabling critical functions to persist despite unpredictable challenges. This framework also accounts for the interdependencies between resilience strategies and environmental outcomes, ensuring that adaptability to unforeseen hazards is balanced with sustainability goals. Resilience characteristics, such as modular design and distributed systems, shape patterns of resource use, energy efficiency, and ecological impacts across systems. By identifying methods to assess and optimize these trade-offs, we provide actionable insights for designing infrastructure that simultaneously enhances resilience and minimizes environmental burdens. Challenges exist in developing methodological foundations for these principles within practical applications to prevent sunk cost and over-constraining operational procedures.

* Corresponding author.
E-mail address: s.a.mitoulis@bham.ac.uk (S.-A. Mitoulis).

https://doi.org/10.1016/j.ijdrr.2025.105535
Received 2 March 2025; Received in revised form 27 April 2025; Accepted 29 April 2025
Available online 30 April 2025

1. Introduction

In an era marked by rapid technological advancements and increasing interconnectivity, the resilience of critical infrastructure has become a central concern. Critical infrastructure encompasses the systems and assets essential to societal functioning, including power grids, transportation networks, communication systems, and water supply networks. These systems underpin national critical functions such as economic stability, public safety, and security, as defined by the Cybersecurity and Infrastructure Security Agency (CISA). Disruptions to infrastructure can cascade across interconnected systems, amplifying socio-economic impacts and exacerbating vulnerabilities. Events such as the 2021 Texas Freeze and the recent unprecedented Iberian Peninsula blackout illustrate how such failures disrupt essential services, revealing the fragility of even advanced systems under compounding stresses.

The landscape of threats to critical infrastructure has expanded, encompassing natural disasters, cyber-attacks, human error, and equipment failures. Many of these threats are novel or evolving, straining traditional resilience strategies that rely on threat-specific preparedness and mitigation. While these approaches have merits, their reliance on predefined scenarios fails to address the full complexity of cascading failures and emerging risks. This gap leaves critical systems unprepared for challenges that fall outside narrowly defined hazard models, resulting in slower recovery and unanticipated vulnerabilities. For instance, the cascading failures during the 2021 Texas power crisis, triggered by extreme cold impacting interdependent natural gas supply and electricity generation systems, highlighted vulnerabilities beyond the scope of traditional single-hazard assessments. A more flexible and comprehensive approach is required—one that accounts for both known and unknown threats.

This paper introduces the concept of threat-agnostic resilience. This refers to a system's ability to maintain critical functions irrespective of the specific nature of the threat. Rather than focusing on individual hazards, this paradigm emphasizes the inherent qualities and capabilities of the system itself, enabling adaptability and robustness in the face of unforeseen challenges. By prioritizing modularity, distributedness, diversity, and plasticity, threat-agnostic resilience fosters systems that can adapt dynamically, limit cascading failures, and recover efficiently [1].

Threat-agnostic resilience is not a static property, but rather a dynamic and evolving capability [2]. As the nature and intensity of threats continue to change over time, so too must the characteristics and network properties of a system's resilience. This type of assessment is an iterative process and must involve stress-testing to optimize and balance the characteristics of a system's resilience [3], such as: instituting modular system connections, distributing system resources to prevent nodal collapse, implementing redundant architectures for backup planning, diversifying agents, and incorporating adaptive response within agents as system plasticity.

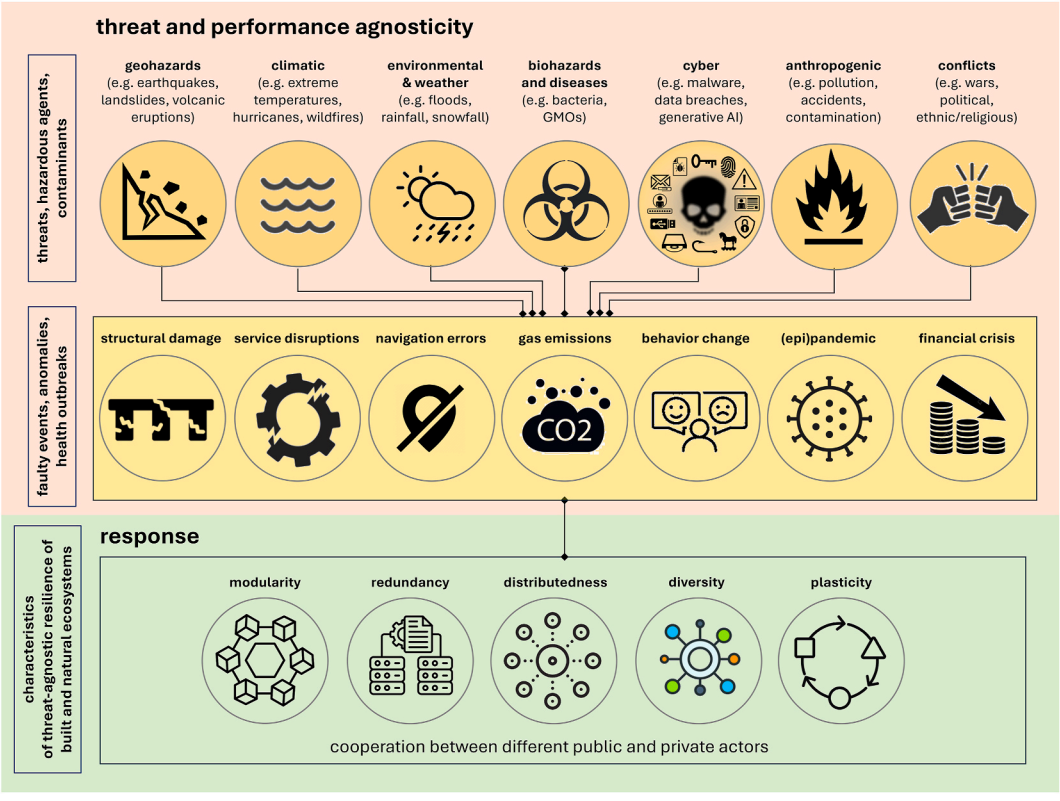


Fig. 1. Framework for assessing and enhancing threat-agnostic resilience of complex systems. Unpredictable threats (orange circles) have a variety of impacts across domains of critical infrastructure (yellow circles). Implementing resilience across domains requires threat-agnostic resilience characteristics (green circles, also described in Fig. 4).

The primary objective of this article is to articulate the characteristics that underpin threat-agnostic resilience and their application to critical infrastructure. We present a framework to evaluate and enhance these characteristics, integrating considerations of operational efficiency and environmental sustainability. While not prescriptive, this framework offers a foundation for tailoring resilience strategies to specific systems, enabling the development of infrastructure that is robust, adaptive, and sustainable in the face of both contemporary and future challenges [4].

To address these limitations, this paper introduces the concept of threat-agnostic resilience, focusing on inherent system characteristics that promote adaptability irrespective of the specific threat origin. This approach complements existing resilience research, which includes broad assessments of the state-of-the-art through bibliometric analysis, reviews of measurement frameworks, and studies focusing on indicator-based assessments [5–7]. While these studies provide valuable context and methods for known risks or specific resilience dimensions, the threat-agnostic framework proposed herein specifically targets the challenge of preparing systems for *unforeseen* or *novel* disruptions by enhancing core adaptive capacities—modularity, distributedness, diversity, and plasticity—and explicitly integrating environmental sustainability considerations.

1.1. Characteristics of threat-agnostic system resilience

The development of threat-agnostic resilience in critical infrastructure systems relies on the identification and cultivation of specific system characteristics. The key characteristics that have emerged include modularity, distributedness, redundancy, diversity, and plasticity. These characteristics, when properly integrated into the design and operation of infrastructure systems, contribute to their ability to maintain functionality and integrity in the face of diverse and unpredictable threats, such as environmental, cyber, anthropogenic, and geopolitical conflicts [3,8,9]. These disruptions cause schisms within infrastructural integrity at various domains, including within physical infrastructure, social response, cyber components, and financial health [10]. While the characteristics of modularity, distributedness, and redundancy contribute collectively to resilience, they represent distinct system properties. **Modularity** specifically refers to the system's decomposability into separable and recompilable units, facilitating containment of failures and targeted repairs or upgrades; its focus is on structural segmentation. **Distributedness**, conversely, pertains to the spatial dispersion and decentralization of critical functions, control, or resources across the network to mitigate reliance on central points; its focus is on avoiding concentration. **Redundancy** involves the deliberate duplication of components or pathways providing identical or similar functions to ensure backup capacity and continuity of service when primary elements fail; its focus is on multiplicity. Although a system might exhibit multiple characteristics simultaneously (e.g., a modular system might also be distributed), understanding their unique conceptual focus is essential for targeted resilience enhancement. The resilience characteristics proposed in this research contribute to maintaining the integrity of infrastructure across each domain despite the unpredictability of threat origin, i.e., threat agnosticity (Fig. 1).

Table 1 presents an overview of each principle of threat-agnostic resilience. The following sections dive into greater detail the components of each principle's definition, practical forms of each principle in critical infrastructure, quantification strategies in

Table 1
Characteristics of threat-agnostic resilience.

Threat-agnostic resilience characteristic			
Definition	Practical examples	Quantification strategies	Contribution to threat agnostic resilience
Modularity			
Degree to which system components can be separated, reengineered and recombined.	Modular design, construction, and repair, baseline training	Modularity and coupling indices, clustering coefficient, average path length	Limits impact of localized failures; facilitates easy replacement and upgrading. Each module is often considered 'plug and play', or easily substituted with minimal startup resources.
Distributedness			
Distribution of system functions across multiple nodes or components, reducing reliance on a central service or authority.	Decentralized functions and control, load balancing, tactical operating procedures	Centrality, clustering coefficient, average path length, diameter	Eliminates single points of failure and enabling local services and responses to maintain system functionality.
Redundancy			
Duplication of critical components or functions to increase capacity and reliability with parallel components or functions (not in series).	Redundant architectures, "N" redundancy, network redundancy, definition of critical skillsets in organizations	Redundancy ratio, connectivity index,	Ensures availability of alternative resources regardless of threat type; provides multiple layers of service and protection.
Diversity			
Inclusion of diverse components or strategies to handle a variety of threats and consequences.	Heterogeneous systems and training lateral thinking	Shannon index, functional diversity index, qualitative indicators	Increases the likelihood of some components surviving or functioning under different threat conditions.
Plasticity			
Ability of a system to adapt its structure or behavior in response to changes in the environment or internal conditions.	Dynamic reconfiguration; system upgrade; versatility	Adaptability index, reconfigurability index, qualitative indicators	Enables dynamic response to unforeseen threats and supports continuous operation by reconfiguring component behavior, resources and strategies.

various fields, and the contribution to threat-agnostic resilience.

1.2. Modularity

Modularity is a key principle in the design of resilient engineered systems (Fig. 4). It allows for the decomposition of complex systems into smaller, more manageable components. Each module can be designed, developed, and tested independently, while still maintaining the ability to integrate seamlessly with other modules to form a cohesive, integral system. This approach enhances the overall resilience of the system by localizing potential failures and enabling rapid recovery through the replacement or repair of individual modules without affecting the entire system and its operations. It is critical to note that modularity, as well as any resilience principle, alone cannot guarantee the resilience of an engineered system to all threats. Specifically, modularity alone may fail to recover from systemic disruption within highly interconnected environments, e.g., common problems such as border conflicts surrounding water scarcity.

In practice, modularity can be achieved through the application of standardized interfaces, protocols, and architectures. These standards ensure interoperability between different modules and facilitate the plug-and-play integration of components from various vendors. For instance, in a modular water distribution system, standardized pipe fittings and valve configurations allow for the easy connection and disconnection of different subsystems, such as treatment plants, storage tanks, and distribution networks. This modularity enables the system to adapt to changing demands and maintain functionality even when individual components fail.

To quantify the modularity of an infrastructure system, network science provides a range of metrics and tools such as the modularity index, coupling index, clustering coefficients, and average path length. The modularity index measures the strength of division of a network into modules or communities, where higher scores indicate connected modules with sparse inter-module connections, which is a desirable property for resilient systems. The coupling index quantifies the degree of interdependence between modules [11], where lower scores suggest modules have limited co-dependence. Clustering coefficients and average path lengths in tandem describe how tightly-knit infrastructure systems are. A high clustering coefficient indicates the presence of functional modules, while a low path length represents efficient resource flow between modules.

Methodologically, calculating metrics like the modularity index or clustering coefficients requires a well-defined network topology of the infrastructure system, typically developed during Step 1 (Critical Function Decomposition) and Step 2 (Network Resilience Characterization) of the framework. These structural metrics offer the advantage of providing objective, quantifiable insights into system segmentation, which aids in identifying potential boundaries for localized failure containment (Step 3). However, a disadvantage is that these static structural measures may not fully capture dynamic interdependencies or the functional consequences of modularity during disruption scenarios, requiring complementary analysis through stress testing (Step 4).

Two benefits of modularity include the ability to scale the system over time and to decouple functions within the infrastructure system. Scalability is particularly important in rapidly growing urban areas, where the infrastructure needs to keep pace with the increasing population, economic activity and changing demand. For example, in a modular transportation system, new bus routes or train lines can be added to the network without disrupting the existing services, thereby enhancing the overall capacity and resilience of the system. Decoupling functions expands system scaling by optimizing parts of the whole, for example, modular power distribution systems can separately optimize generation, transmission, and distribution systems without requiring complete system overhauls.

In social and organizational systems, modularity refers to the ability of different social groups or organizations to operate independently while still contributing to the overall resilience of the community, allowing for targeted interventions and support. For example, conducting community workshops to train local organizations on independent crisis management strategies that can be coordinated during a larger emergency.

1.3. Distributedness

Where modularity refers to the capacity of engineered systems to operate in discrete, self-contained compartments, distributedness refers to the allocation of system functions and governance across multiple dispersed nodes or components (Fig. 4). This design reduces reliance on a central authority or single point of control, enhancing the system's ability to operate independently in different locations. Distributedness also enables the scalability of infrastructure systems, where new nodes or components can be added to the network without requiring significant modifications to the existing architecture. This capability allows for the gradual expansion and upgrading of the system over time, in response to changing demands or technological advancements.

In the context of practical infrastructure systems, distributedness can be achieved through the implementation of distributed control architectures, such as multi-agent systems [12], peer-to-peer networks, or blockchain-based platforms. Distributed optimization algorithms, such as consensus-based methods or alternating direction method of multipliers (ADMM), can be applied to achieve system-wide objectives, such as energy efficiency or load balancing [13]. Within a fully distributed infrastructure system, each node or component has the capacity to process information, make decisions, and coordinate actions with other nodes in the network. For example, in a distributed water management system or transport system, smart sensors and actuators can be deployed throughout the network to monitor service levels, such as water quality or traffic conditions in real-time, without relying on a central control room.

To quantify the degree of distributedness in an infrastructure system, various metrics from network science can be applied. One commonly used metric is the degree of centrality, which measures the extent to which the functionality of the system depends on a few central nodes. A lower degree of centrality indicates a more distributed system, where the importance and influence of individual nodes are more evenly spread across the network. Similar to modularity, the clustering coefficient and average path length provide location and commodity-based views of infrastructure distribution. Furthermore, network diameter represents the maximum distance

between any pair of nodes. A distributed system with a low average path length and a small diameter can facilitate the rapid dissemination of information and the efficient coordination of actions across the network, even in the presence of failures or disruptions.

Applying centrality measures or calculating network diameter (Steps 2/3) relies on detailed network connectivity data. The advantage of these metrics lies in identifying potential single points of failure (high centrality nodes) or bottlenecks in resource or information flow (high diameter or path length). A limitation is that topological distributedness does not guarantee functional resilience; operational protocols and resource allocation strategies, explored during Step 4 (Stress Testing), are also critical for realizing the benefits of a distributed structure.

One of the key advantages of distributedness in infrastructure systems is the increased resilience to failures and attacks. In a centralized system, a failure or compromise of the central node can lead to the collapse of the entire system. In contrast, a distributed system can continue to function even if some of its nodes are damaged or disconnected, as the remaining nodes can compensate for the loss in service and control and maintain the system's overall functionality at acceptable levels. This resilience is particularly important in the face of natural disasters, cyber-attacks, or other disruptions that can target specific components of the infrastructure.

In social and organizational systems, distributedness means the dispersion of decision-making power and resources across various stakeholders, enhancing collective action and reducing dependency on a central authority. For example**:** organizing leadership training programs for community leaders to empower decentralized decision-making and resource allocation during crises.

1.4. Redundancy

Redundancy ensures the availability of backup components or functions in the event of failures or disruptions [14]. For engineered infrastructure, redundancy can be achieved through the duplication or replication of critical assets, such as power generators, communication links, or water treatment plants (Fig. 4). This redundancy allows the system to maintain its functionality even when some components fail, by seamlessly switching to the backup components or rerouting the flow of resources through alternative paths of similar constitution or service delivery.

The implementation of redundancy in infrastructure systems can take various forms, depending on the specific requirements and constraints of the system. One common approach is the use of N+1 or N+2 redundancy, where N represents the number of components required for normal operation, and the additional components serve as backups [15]. For example, in a data center with N+1 redundancy, if one server fails, the backup server can immediately take over its functions without interrupting the services provided by the data center. Redundancy can also be achieved at the system level, by providing multiple alternative paths or routes for the flow of resources, such as electricity, transportation of people and goods, water, or data. This type of redundancy, known as network redundancy or path diversity, enhances the resilience of the system to link failures or congestion [16]. In a transportation network, for instance, the presence of multiple alternative routes between origin and destination points allows for the rerouting of traffic in the event of road closures or accidents. Similarly, in a communication network, the deployment of redundant fiber optic cables or wireless links ensures the continuity of data transmission, even if some links are damaged or degraded.

To quantify the level of redundancy in an infrastructure system, several metrics can be employed. One widely used metric is the redundancy ratio, which is defined as the ratio of the number of redundant components to the total number of components in the system [17]. A higher redundancy ratio indicates a more redundant system, which is generally more resilient to failures. For example, a power grid with a redundancy ratio of 0.2 means that 20 % of its components are redundant, providing a significant buffer against potential failures. Another important metric for assessing the redundancy of an infrastructure system is the connectivity index, which measures the number of independent paths between any two nodes in the network. A higher connectivity index suggests a more redundant and resilient system, as it indicates the presence of multiple alternative routes for the flow of resources [18].

Quantifying redundancy through ratios or connectivity indices (Step 3) provides a straightforward measure of backup capacity, clearly linking structural duplication to the potential for maintaining function during component failure. Disadvantages include the potential cost implications associated with redundant components (often requiring trade-off analysis during design and Step 4 simulations) and the fact that simple component duplication does not guarantee resilience against systemic disruptions or common-mode failures, which might necessitate more diverse redundancy strategies.

An advantage of redundancy to infrastructure resilience is the presence of physical back-ups as responsory action to disruption but is presented with opportunity cost. In general, higher levels of redundancy provide greater resilience, but also incur higher costs in terms of capital investment, maintenance, and operation [15,19]. Therefore, the design of redundant systems should involve a trade-off analysis between the benefits of increased resilience and the associated costs, taking into account the specific requirements and constraints of the system.

In social and organizational systems, redundancy refers to the presence of multiple social networks and support mechanisms that can provide assistance and resources during disruptions, ensuring community resilience. Example: Conducting training sessions for multiple community volunteers to establish and manage emergency shelters, ensuring that if one volunteer is unavailable, others can seamlessly take over the responsibilities. Additionally, training multiple personnel for the same task ensures that there are always qualified individuals available to perform critical functions, thereby enhancing the overall resilience of the community.

1.5. Diversity

In the context of infrastructure systems, diversity refers to the incorporation of heterogeneous components, technologies, and operational strategies, which collectively enhance the system's ability to withstand disruptions and maintain its functionality under

varying conditions [20]. Diversity is a critical characteristic of resilient engineered systems, as it enables them to cope with a wide range of threats and uncertainties [21].

Diversity can be achieved in infrastructure systems through varying source providers, incorporating heterogeneous components and materials, and assimilating operational strategies and control mechanisms (Fig. 4). Varying source providers within power generation might include a diverse mix of renewable energy sources, such as solar, wind, and hydro, can be integrated alongside conventional generators, providing a hedge against market fluctuations and geopolitical risks [22]. Implementing various infrastructural materials or ways of throughput also increases resilience to single modes of failure, such as by incorporating heterogeneous pipe materials in water distribution networks [23,24] or adopting multiple transportation networks within smart cities. Diversifying control strategies [25], such as in distributed power generation from smart grids or adaptive signal control in transportation engineering, can minimize strain on the reference system during peak periods and allow for continuous flow of goods, people, or resources [26].

To quantify the level of diversity in an infrastructure system, metrics such as the Shannon index and functional diversity index are viable. The Shannon index measures the richness and evenness of different types of components in the system [27], and while the Shannon index is commonly used in ecology, it can be used within infrastructure to assess the impact of infrastructure improvements on environmental diversity [28]. A higher Shannon diversity index indicates a more diverse system, which is generally more resilient to threats and uncertainties. In parallel, the functional diversity index measures the variety and distribution of different functional attributes, such as the capacity, efficiency, or reliability of each component or subsystem [29]. A higher functional diversity index suggests a more versatile and adaptable system, which can maintain its performance under different conditions and requirements.

Using indices like the Shannon index or functional diversity index (Step 3) helps quantify the variety of components, technologies, or strategies within the system, providing an advantage by capturing heterogeneity linked to resilience against varied threats. However, quantifying functional diversity can be methodologically complex, requiring careful definition of relevant functional attributes and potentially significant data collection. Furthermore, maximizing diversity may sometimes conflict with goals like standardization or efficiency, representing a key trade-off to be evaluated, potentially using the stress-testing approach in Step 4.

In addition to these quantitative metrics, the assessment of diversity in infrastructure systems should also consider the qualitative aspects of the system's resilience [30]. For example, the compatibility and interoperability of different components and technologies should be evaluated, to ensure that they can work together seamlessly and efficiently [31]. The scalability of the system should also be assessed, to determine its ability to accommodate future growth and adapt to changing demands.

An advantage of diversity within infrastructure systems is the increased likelihood of system survival and operation to any disruption. By embracing diversity, infrastructure systems can reduce their reliance on any single component or technology and improve their adaptability to changing environments. However, overly diverse systems can limit other resilience characteristics, such as modularity and plasticity, potentially making improvements to system capacity and quality more laborious and resource-intensive.

In social and organizational systems, diversity refers to the inclusion of different perspectives, skills, and resources within a community of practice, which enhances problem-solving capabilities and adaptability to changing conditions. In other words, the application of training to enhance critical and lateral thinking in which the diversity of perspectives can support the understanding of complexity. For example, hosting cross-disciplinary or cross sectoral workshops to train community members on leveraging diverse skills and perspectives for effective crisis response.

1.6. Plasticity

Plasticity enables engineered systems to adapt their structure or behavior in response to changing conditions (Fig. 4). While plasticity holds definitions in other fields such as materials science, in the context of infrastructure systems for this research, plasticity refers to the ability of the system to modify its configuration, operations, or performance based on the dynamic variations in the environment, user demands, or internal states without further degradation of the system's performance after a disruption. Other terms in network science and ecology that are adjacent to this definition include suppleness (the ability of a network to maintain form under stress [32]) and adaptability (actors' influence on resilience within a system [33]). However, the definition of plasticity posited by this paper combines the influence of both *actor* and *network* to impose systemwide change before, during, or after a disruption.

Practical applications of plasticity in infrastructure systems includes adaptive control strategies, reconfigurable architectures, and mechanisms for self-organization. Adaptive control involves real-time monitoring and adjustment of system parameters based on feedback loops and learning algorithms [34]. For example, in a smart energy grid, adaptive control can be used to dynamically balance the supply and demand of electricity, by optimizing the dispatch of generators, the configuration of transmission lines, or the pricing of energy services [35]. Reconfigurable architectures allow the system to change its structure or topology, by adding, removing, or rearranging its components or connections. For instance, in a modular transportation network of high plasticity, reconfigurable architectures can be used to dynamically adjust the layout of roads, bridges, or terminals, based on the shifting patterns of traffic flow, land use, or urban development [36]. Self-organizing mechanisms rely on the local interactions and autonomous behaviors of the system components, which collectively give rise to the emergence of global patterns and functions. For example, in a decentralized water distribution network, self-organizing mechanisms can be used to enable the autonomous coordination of pumps, valves, and tanks, based on the local sensing and communication of water quality, pressure, or demand.

To assess the plasticity of an infrastructure system, metrics, such as the adaptability index and reconfigurability index can be adopted. The adaptability index measures the degree to which the system can modify its structure or behavior in response to perturbations [37]. It is a function of the range and speed of the system's responses, as well as the effectiveness and efficiency of the adaptations. A higher adaptability index indicates a more plastic system, which can better cope with the changing conditions and maintain its performance over time. The reconfigurability index quantifies the ease and speed with which the system can be

reconfigured to meet new requirements or recover from failures [38] and is a function of the number and diversity of the system's configurations, as well as the time and cost required for the reconfigurations. A higher reconfigurability index suggests a more flexible, responsive system, such as highway segments after a major flood.

Assessing plasticity via adaptability or reconfigurability indices (Step 3) aims to capture the system's dynamic response potential, directly focusing on adaptive capacity. Key methodological challenges include the difficulty in defining objective, universally applicable indices for complex, unique infrastructure systems and the difficulty of validating these measures without extensive simulation or real-world performance data (Step 4). Consequently, qualitative assessments of adaptive processes and mechanisms often remain crucial for understanding a system's true plasticity.

In addition to these quantitative metrics, the assessment of plasticity in infrastructure systems should also consider the qualitative aspects of the system's resilience. For example, the robustness and scalability of the adaptive control strategies should be evaluated, to ensure that they can handle a wide range of perturbations and uncertainties, without leading to unintended consequences or cascading failures. The interoperability and compatibility of the reconfigurable architectures should also be assessed, to ensure that they can seamlessly integrate with the existing systems and standards, while enabling the smooth transition between different configurations.

Plasticity offers significant advantages for resilience, enabling systems to adapt dynamically to changing conditions through both resilience-by-design (inherently adaptive architectures) and resilience-by-design (active reconfiguration) principles. This capacity allows systems to modify configurations, operations, or performance levels in response to disruptions or evolving environmental demands, potentially reducing recovery times and maintaining critical functions under unforeseen circumstances. However, plasticity is not universally or unconditionally beneficial and introduces potential trade-offs (nor is any other characteristic universally and unconditionally beneficial, given resource constraints and operating requirements). High levels of plasticity can increase system complexity, making design, control, and prediction more challenging. The process of adaptation or reconfiguration itself might introduce transient periods of instability or reduced performance. Furthermore, maintaining the capacity for plasticity often requires significant investment in monitoring systems, diverse component inventories, advanced control algorithms, and skilled personnel, which may compete with other resource allocation priorities. Therefore, the optimal degree of plasticity must be carefully evaluated for each specific infrastructure system, balancing the benefits of adaptive capacity against potential increases in complexity, cost, and operational uncertainty.

Plastic infrastructure configurations are advantageous through resilience-by-design and resilience-by-intervention principles [39, 40]. By incorporating system architectures that are innately adaptive, infrastructure layouts can inherently self-organize and can implement agents for response that presume multiple roles. However, a balancing point for consideration by practitioners might be the quality of adaptive architectures and the time-to-survive [41] during a recombination period for the uptake of new roles by plastic agents.

In social and organizational systems, plasticity refers to the capacity of social networks and institutions to adapt their roles, behaviors, and interactions in response to evolving challenges, ensuring sustained community resilience. Examples include scenario-based training exercises for community leaders to practice adaptive responses to prolonged crises, such as shifting roles and responsibilities.

2. A framework for adopting resilience characteristics within critical infrastructure systems and environment

To operationalize threat-agnostic resilience, we propose a multi-step framework that integrates network science, systems engineering principles, and environmental considerations (Fig. 2). This approach balances the need for robust, adaptable infrastructure with the imperative to minimize environmental impacts, ensuring that resilience strategies are both effective and sustainable.

The first step involves a comprehensive analysis of the infrastructure system to identify its critical functions, the infrastructure supporting them, and the associated environmental dependencies. As defined by CISA, critical functions are the functions of government and the private sector that are paramount to a nation's security, economic health, and public health and are commonly upheld by critical infrastructure [42]. Evaluating critical infrastructure in the broader service-level lens begins an assessment of interconnectivity within critical infrastructure across sectors, which is crucial quantifying resilience within a network. For example, a

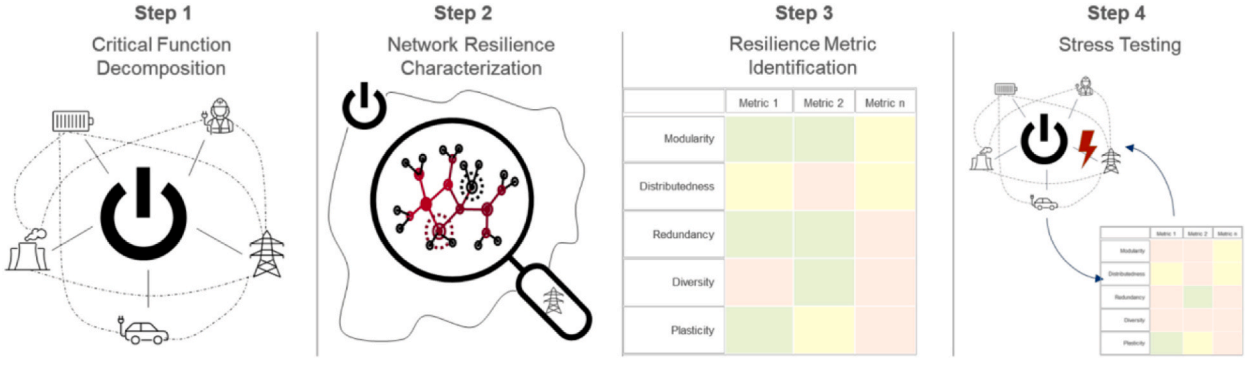


Fig. 2. Placing threat-agnostic resilience characteristics within infrastructural critical functions through stress testing.

power grid's critical functions include generation, transmission, and distribution, but these are also tightly linked to land use, water consumption, and greenhouse gas emissions. By mapping these functions, their interconnections, and their environmental externalities, planners can better understand the system's vulnerabilities, potential failure points, and ecological impacts.

In this phase, understanding critical functions requires considering how technical vulnerabilities interact with their operational context. This includes examining the organizational sphere (processes and procedures), the social and behavioural sphere (culture and perceptions), and the political and governance sphere (legal frameworks and compliance). In other words, understanding the system involves characterizing and assessing "soft" functions that could be preconditions and potential single points of failure, compromising capacity deployment across operational scales [43]. In a complex environment characterized by multiple stakeholders and lack of information, or patterns of misinformation, assessing interdependencies and weaknesses between technical elements and governance functions becomes the driver of internal and external crisis coordination.

The relevance of these interactions is particularly significant when considering high-impact, low-probability events (HILPs), or outlier events, which are distinguished by "a lack of precedence and high levels of uncertainty in their predictability and combinations of effects, often coming as surprises or shocks" [44]. HILPs may not meet the defined thresholds for activating mitigation actions, but they can still affect operations with the range of scenario that in which they are manifested. Aligning organizations and networks, both internally and externally, is crucial to ensure flexibility of response while strengthening coordination and developing adaptable response plans enable organizations to better navigate unexpected disruptions, maintaining resilience and operational continuity.

The next step associates each critical function with the resilience characteristics that most significantly support its operation and its environmental performance. This association is not necessarily one-to-one; multiple characteristics may bolster a single function, and each characteristic may affect environmental outcomes differently. For instance, distributed energy systems enhance resilience to localized failures while reducing transmission losses, but they may require higher initial investments in renewable energy sources and storage systems. Similarly, modular water distribution systems can localize disruptions and improve resource efficiency, minimizing water loss and energy use during repairs. By explicitly linking these characteristics to specific functions, we can develop a more targeted approach to enhancing system resilience.

To quantify the degree to which resilience characteristics support both critical functions and environmental goals, specific metrics must be developed in the third step of the framework. These metrics should capture not only operational efficiency and robustness but also environmental trade-offs, such as embodied carbon, resource consumption, or land-use impacts. For instance, modularity in a transportation network might be measured by the number of independent sub-networks, their energy efficiency, and the potential reduction in urban sprawl. Similarly, redundancy in water systems could be evaluated through water-use efficiency, energy intensity, and ecological impacts on watershed systems. These metrics provide a basis for assessing the co-benefits and trade-offs between resilience and environmental sustainability.

The fourth step involves stress testing and simulation techniques to evaluate system performance under a wide range of conditions, including both operational disruptions and environmental stressors. These stressors could include random node or link failures, as well as climate-related shocks such as heatwaves, flooding, or drought. Advanced simulation methods, such as agent-based modeling Monte Carlo methods [45], or life cycle-based environmental impact assessment, can help predict the system's behavior under diverse scenarios, varying demand load conditions, or predefined threat scenarios. This step enables planners to identify vulnerabilities, optimize resilience strategies, and evaluate their environmental ramifications in an integrated manner.

Applying the threat-agnostic resilience framework requires acknowledging the different analytical demands posed by technical versus social or behavioral disruptions. While technical failures (e.g., component damage, network outages) are often amenable to quantitative characterization and metric identification using network science tools (Steps 3 and 4 of the framework), assessing social dimensions presents distinct challenges. Evaluating aspects such as organizational response capacity, community adaptive behaviors, or shifts in public perception often necessitates the integration of qualitative indicators, as noted in Table 1, and mixed-methods

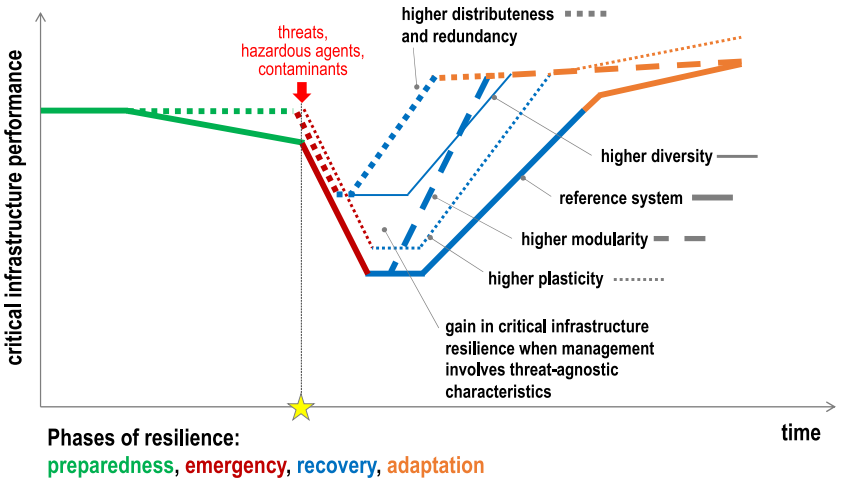


Fig. 3. The positive impact of the five characteristics of threat-agnostic resilience on critical infrastructure performance.

approaches. Techniques like stakeholder analysis, scenario-based workshops, expert elicitation, and case study methodologies may be required alongside, or in place of, purely quantitative metrics to adequately characterize resilience in the face of social disruptions. Consequently, a comprehensive evaluation of resilience within complex socio-technical systems inherently demands interdisciplinary perspectives, combining engineering and network science insights with expertise from social sciences, organizational studies, and governance research.

This framework provides a comprehensive method for aligning engineered system resilience objectives with environmental

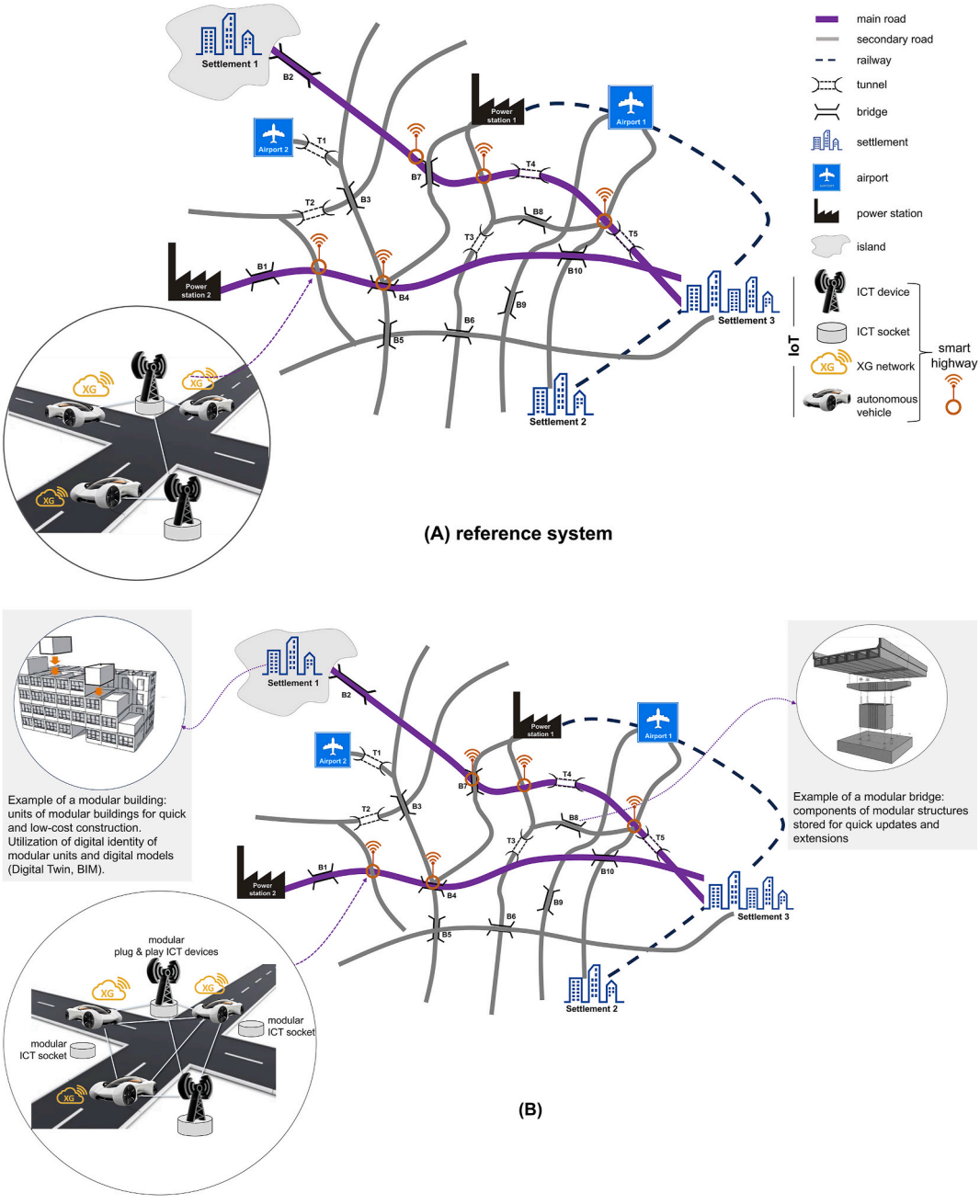


Fig. 4. Threat-agnostic resilience within critical infrastructure. Panel A presents a reference system of a smart transportation network connecting urban and island settlements, airports, and power stations. Panel B, increases modularity by implementing modular construction units and buildings, and modular ICT components. Panel C implements lower distributedness by removing a power station and airport, while there is only one smart highway within the network. Panel D lowers redundancy by removing smart roadways, power stations, and airports. Panel E increases diversity by varying transportation modes, construction materials based on local infrastructural use and bridge design, and alternative ICT units. Panel F increases plasticity by adding new transportation and communication (ICT) modes.

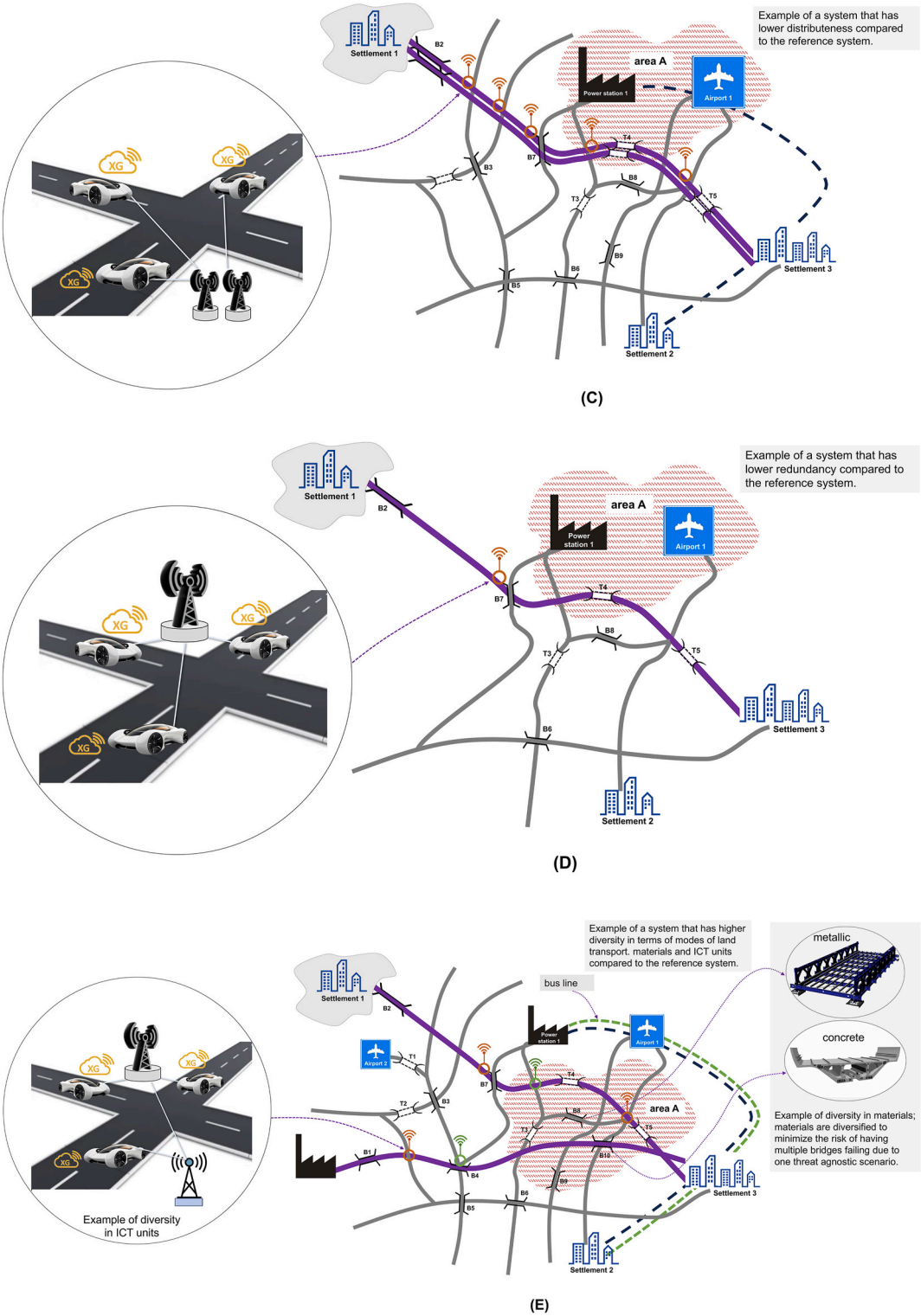


Fig. 4. (*continued*).

sustainability, regardless of threat context. By focusing on critical functions, their supporting characteristics, and their environmental context, it offers a scalable and adaptable approach for infrastructure systems across sectors. It enables system designers and operators to develop resilience strategies that are robust to dynamic threats while minimizing resource consumption and ecological degradation.

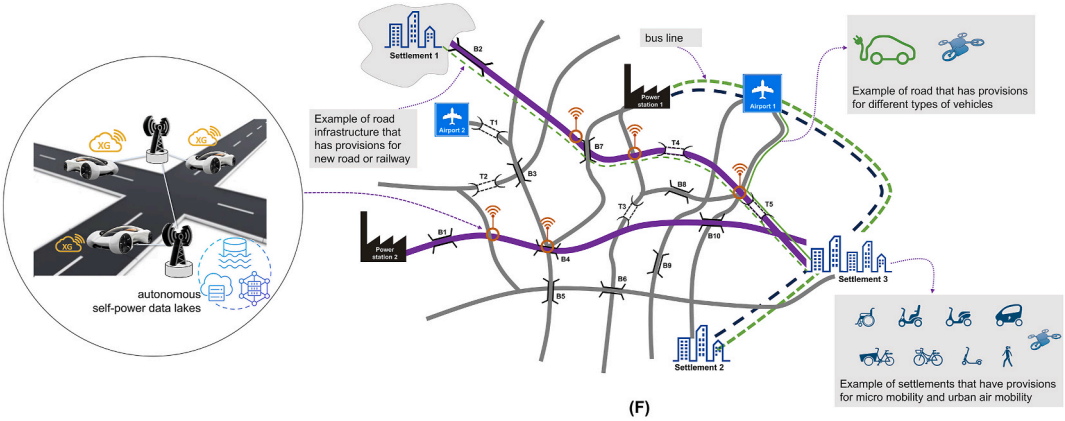


Fig. 4. (*continued*).

By focusing on critical functions and their supporting characteristics, it provides a flexible approach that can adapt to emerging and unforeseen challenges. Moreover, it enables system designers and operators to identify key leverage points for enhancing resilience across multiple dimensions simultaneously. This approach is particularly valuable in the context of complex, interconnected infrastructure systems, where traditional risk-based approaches may be insufficient to capture the full range of potential disruptions and their cascading effects.

The intricate interplay of threat-agnostic resilience configurations within critical functions, as depicted in Fig. 3, reveals a narrative of how complex infrastructure systems can mitigate losses, expedite recovery, and enhance adaptive capacity of the critical functions provided. Far from operating in isolation, these principles form a synergistic framework that amplifies the overall resilience of critical systems.

The reference system, depicted by a solid blue line, serves as a baseline for comparison, exhibiting a typical response pattern to disruption. This pattern is characterized by a sharp decline in performance following a disruptive event, marked by a yellow star, followed by a gradual recovery. Such behavior aligns with classical resilience models proposed by Holling [46] in 1973 and further developed by Walker et al. [33] in 2004. The reference system's trajectory enables a comparative analysis of systems enhanced with specific resilience characteristics, providing insights into the effectiveness of various resilience strategies.

Higher modularity, represented by a dashed blue line, shows an intermediate response profile. The modular system experiences a less severe performance drop compared to the reference system and recovers at a moderate pace. Modular design facilitates infrastructure system mission execution amidst disruption, ranging from mitigating transit system delays during peak disruption periods [47], to rerouting of shipments in supply chains [48]. Likewise, the system with higher plasticity, depicted by a dotted blue line, exhibits a unique response profile characterized by a moderate initial performance decline but a rapid recovery. This behavior underscores plasticity's role in enabling quick system reconfiguration and adaptation to post-disruption conditions [49,50].

Systems with higher distributedness and redundancy, represented by a dotted blue line, demonstrate the most robust response to disruption. These systems experience a less severe initial performance drop and recover more rapidly, quickly surpassing the reference system's recovery trajectory. This superior performance can be attributed to the spatial dispersion of critical components and the availability of backup resources. Notable examples include municipal water systems, where centralization of piped water supply and sewer networks requiring central control are prone to systemic disruption from relatively minor disruptions to water quality that could often be addressed through local water treatment and management interventions [51]. The collective effect of these characteristics mitigates the impact of localized disruptions and accelerates the restoration process, highlighting the importance of decentralized design in critical infrastructure.

The system characterized by higher diversity, illustrated by a solid orange line, initially experiences a decline similar to the reference system with smaller losses and exhibits a steeper recovery curve. This behavior suggests that diverse systems, while not necessarily more resistant to initial shocks, possess a greater capacity for rapid adaptation and recovery. Emerging examples include municipal and regional energy grids, where systems with diverse energy sources recovered faster from major disruptions compared to homogeneous systems [52]. The varied resources and operational strategies inherent in diverse systems provide multiple pathways for recovery, enhancing overall system resilience [53].

Below, Fig. 4 provides a comprehensive visual representation of how the principles of threat-agnostic resilience can be applied to complex, interdependent infrastructure systems. By illustrating various configurations of a critical infrastructure network, the figure demonstrates the impact of different resilience characteristics on system performance and adaptability in the face of unknown threats.

Panel A presents the reference system, which serves as a baseline for comparison. This configuration represents a typical infrastructure network, comprising multiple settlements, airports, power stations, and smart transportation links. The reference system exhibits a balanced approach to resilience, with a moderate level of redundancy, diversity, and distributedness. This baseline configuration allows us to evaluate how changes in system design can enhance or diminish overall resilience.

Panel B showcases a system with enhanced modularity compared to the reference system. In this configuration, we observe a more segmented structure, with clearly defined sub-systems of transport and ICT infrastructure that can operate independently, if needed.

This design allows for localized management of resources and risks, ensuring that a disruption in one part of the system does not necessarily compromise the entire network. Second, the design facilitates easier maintenance and upgrades, as individual modules (units and components) can be taken offline for repairs or improvements without affecting the whole system (plug-and-play modules and ICT sockets) [54]. An example of that is California's Interstate 210 connected corridor that integrates modular ICT systems for traffic management, such as vehicle-to-infrastructure (V2I) communication units and dynamic message signs. Each segment of the system can function autonomously, ensuring that disruptions in one part do not cascade across the transportation network [55].

Panel C illustrates a system with reduced distributedness compared to the reference system. In this scenario, critical functions and control centers are concentrated in fewer locations, presenting a stark contrast to the distributed approach of threat-agnostic resilience. While this centralized approach may offer some efficiency gains under normal operating conditions [56], it significantly compromises the system's resilience to unknown threats. The concentration of critical assets in Panel C creates a potential single point of failure, making the entire system vulnerable to localized disruptions. For instance, if area A (as indicated in the figure) is affected by an unforeseen event, the impact on the system could be far-reaching and limit future adaptive capabilities. For example, in 2015, a SCADA failure in the North-Central railway zone of Indian Railways caused widespread power disruptions, halting train operations on major routes, including the New Delhi-Howrah and New Delhi-Mumbai corridors. The failure was traced to a central server issue, demonstrating the vulnerabilities of centralized control systems [57].

Panel D depicts a system with diminished redundancy compared to the reference case with area A illustrating a geospatial disruption concern for the system. In this configuration, we observe fewer backup components of transportation and ICT and alternative service routes. The system features only one airport and one power station, in contrast to the two of each, present in the reference system. The overall cost of the system is lower, in terms of construction and maintenance. However, its resilience is critically low. With fewer alternative paths and backup components, the system's ability to maintain functionality during disruptions is severely compromised. The lack of redundancy, specifically in area A, not only affects the system's ability to withstand disruptions but also impacts its recovery capacity and reinstatement of communications. With fewer alternative resources available, the time and effort required to restore normal operations after a disruptive event would likely increase significantly. In January 2022, a severe snowstorm in Athens led to thousands of motorists being stranded on the Attiki Odos highway. The lack of redundancy in the highway's emergency response systems resulted in a slow recovery, compromising the resilience of the transportation network [58].

Panel E focuses on the principle of diversity, showcasing a system with varied modes of transportation compared to the reference system and more diverse construction materials. The increase of transportation options in Panel E enhances the system's flexibility in responding to disruptions. For instance, if road networks are compromised due to an unforeseen event, the absence of alternative transportation modes could lead to significant isolation of certain settlements. Furthermore, Panel E hints at the importance of diversity at the component and material level. The example of constructing bridges using different materials, such as metallic and concrete, illustrates how diversity can enhance resilience against specific threats, and similarly, diverse ICT and transportation options during disruptions lead to increased systemic resilience.

Panel F illustrates a system with greater plasticity compared to the reference case to accommodate better mobility through designated infrastructure. The connection between settlement 3 and airport 1 is enhanced with additional provisions to accommodate different types of mobility solutions. This flexibility allows the system to integrate new transportation technologies or adjust to changing travel patterns without requiring a complete overhaul of existing infrastructure. Similarly, the link between settlements 1 and 3 is designed with space and provisions for future expansion, such as the addition of a new road or railway. This foresight in planning enables the system to evolve organically in response to changing demands or technological advancements. A recent example of resilience demonstrated by shifting from public transportation to micro-mobility is the adaptation seen during the COVID-19 pandemic [59]. Another example is the provision of portable ICT sockets and/or power supply units (batteries) that can facilitate quick recovery.

3. Discussion

The analysis of threat-agnostic resilience characteristics and their application to critical infrastructure systems reveals several key insights with significant implications for infrastructure planning, design, and management. The rise of hybrid threats (e.g., socio-technical) against a range of emerging environmental threats call for threat-agnostic approaches within infrastructure to prevent catastrophic failures [60,61]. Insights from network science provide the tools and methodologies to analyze and understand the structure, dynamics, and resilience of infrastructure [62–65]. By focusing on fundamental resilience characteristics through network science rather than specific threat scenarios, this approach offers a more comprehensive and flexible strategy for enhancing infrastructure performance across a wide range of potential disruptions which may not be identified by threat-aware assessments [66,67].

One of the key advantages of the threat-agnostic approach lies in its scalability and adaptability across diverse infrastructure sectors and geographical contexts. Whether applied to urban water systems, power grids, or transportation networks, the principles of threat-agnostic resilience provide a universal framework for improvement. This universality is particularly valuable for policymakers and infrastructure planners tasked with developing long-term strategies that can withstand evolving threats and changing societal needs. Moreover, the approach facilitates cross-sector collaboration and knowledge transfer, as resilience strategies developed for one infrastructure type can often be adapted and applied to others. By promoting a common language and set of principles for quantifiable and benchmarkable resilience, the threat-agnostic approach enables more effective coordination among different stakeholders involved in infrastructure development and management.

The applicability of the threat-agnostic resilience characteristics extends across different scales of governance, see Fig. 5. Modularity, distributedness, diversity, and plasticity manifest and can be operationalized distinctively at local, regional, and national levels.

For example, modularity at the local scale might involve the design of independent community shelters or microgrids, whereas at the national scale, it could relate to the capability to isolate and operate separable segments of the power grid or transportation networks. Similarly, distributedness could refer to dispersed local resources or decentralized national command structures. The framework presented, particularly the initial steps involving Critical Function Decomposition and Resilience Metric Identification, offers a structured approach to facilitate dialogue among diverse stakeholders. This process can help align potentially competing priorities, such as balancing specific resilience investments against broader community development goals or operational efficiencies. Furthermore, integrating an assessment of 'soft' functional failures—those related to governance limitations, organizational procedures, or coordination challenges—is crucial. Such failures can act as hidden vulnerabilities or single points of failure within the socio-technical system. Explicitly considering these governance and organizational dimensions alongside the technical characteristics is necessary for managing emergent behaviors effectively and aligning resilience efforts across multiple scales and stakeholder groups.

For infrastructure operators and managers, the threat-agnostic approach offers a more proactive stance on resilience, both for engineering design specification, as well as anticipating environmental challenges through the coming decades. Rather than reactively addressing specific vulnerabilities as they are identified, this methodology encourages the continuous enhancement of system-wide resilience characteristics. This shift in focus can lead to more efficient resource allocation and a more holistic approach to risk

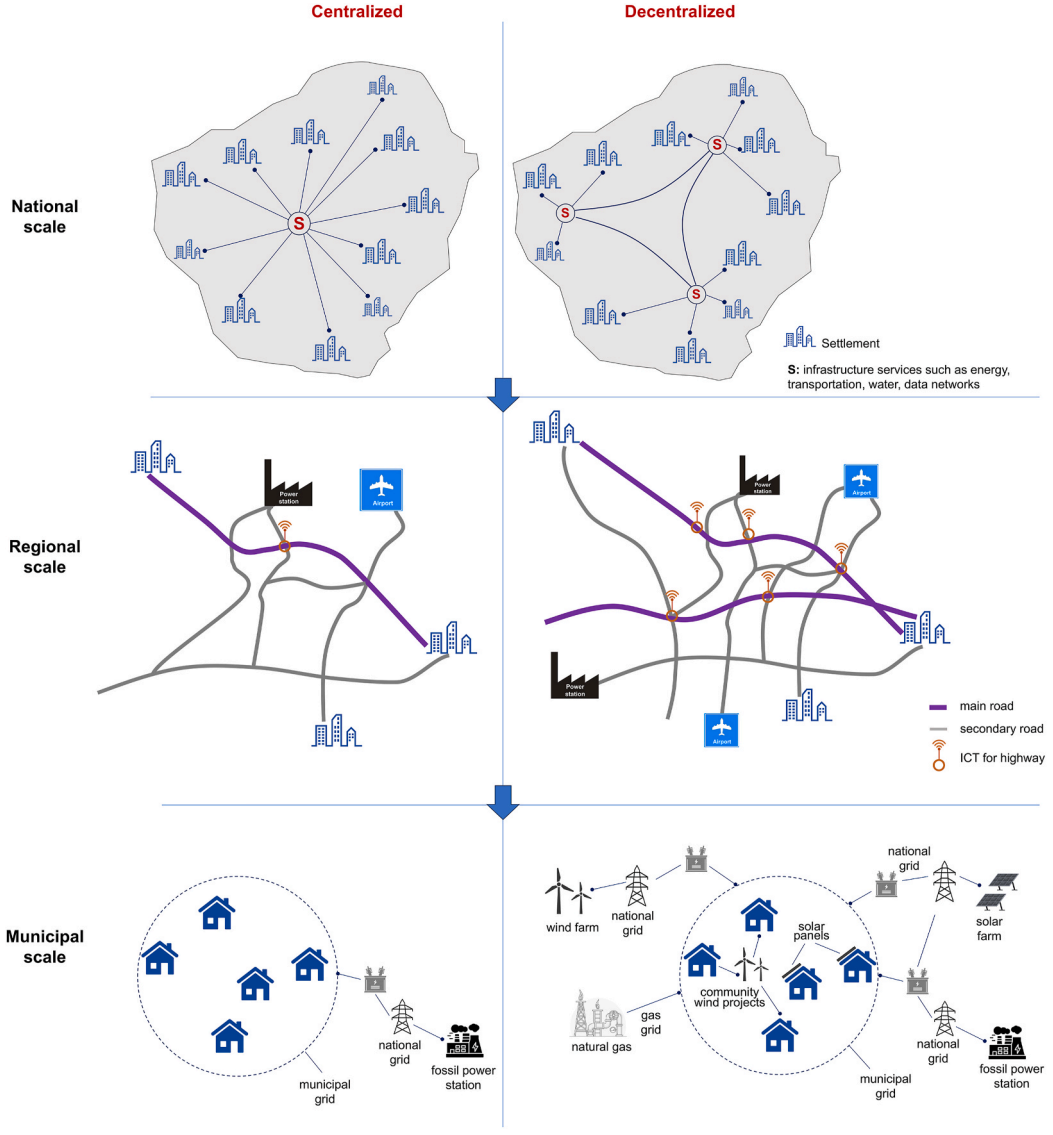


Fig. 5. An illustrative example and brief case comparison demonstrating how the framework could be adapted across different governance contexts. The figure contrasts centralised (S) and decentralised (s) infrastructure services—such as energy, transportation, and data networks—across national, regional, and municipal scales. Examples include fossil power stations connected to national grids versus community-level solar and wind systems linked to municipal grids.

management. By prioritizing system attributes, such as modularity and plasticity, operators can create infrastructure that is inherently more adaptable to changing conditions and emerging threats. Equally, investors, insurers, and financial institutions stand to gain significant benefits from the adoption of a threat-agnostic approach to infrastructure resilience. By evaluating infrastructure projects through these lens, they can make more informed decisions about long-term viability and return on investment. Projects that demonstrate high levels of modularity, distributedness, redundancy, diversity, and plasticity may be viewed as more robust investments in an uncertain future. This perspective can lead to a shift in investment strategies, favoring projects that prioritize long-term resilience over short-term efficiency gains. Additionally, the threat-agnostic approach provides a more comprehensive framework for assessing and pricing risk in infrastructure investments, potentially leading to more accurate valuation of assets and more efficient allocation of capital in the infrastructure sector.

As data sensing infrastructure improves, the continuous monitoring and improvement of threat-agnostic resilience characteristics for long-term infrastructure health. The performance and condition of the system should be regularly assessed, using advanced sensing and data analytics technologies, to detect any potential vulnerabilities or inefficiencies [68]. The system should also be periodically updated and upgraded, incorporating new technologies and best practices, to keep pace with the evolving threats and opportunities in the environment and inform preparedness.

Together with the technical component of infrastructure, further considerations must be attributed to the "soft" dimension of critical services mentioned earlier in the papers.

The scalability of the framework across different scales of governance and decision-making is associated with the principle that the failure of critical services can be rooted in positive and negative feedback loops that defines crisis dynamics, from lack of well-defined procedures to mismanagement [69]. In particular, the complexities introduced by emergent behaviors at varying scales-local, state, and national-can imply the existence of single point of failures in the different levels of organizational sphere, the social and behavioral sphere, and the political and governance sphere, which can then align and trigger cascading effects that progressively escalate [70]. Indeed, governance scale and levels can be seen as critical consideration of shaping resilience priorities, trade-offs, and implementation that affect organizations and how their critical services level [71]. At the local level, governance behaviors often prioritize immediate and tangible resilience measures that directly impact community members or the tactical level of organizations. These measures may include emergency or continuity response plans, local infrastructure improvements, and community engagement initiatives.

However, local governance may face trade-offs such as limited resources and the need to balance short-term and long-term resilience goals [72]. Regional governance tends to focus on coordinating efforts across multiple localities, leading to more comprehensive and integrated resilience strategies including or excluding the understanding critical services. This level of governance can facilitate the sharing of resources and best practices, but it also introduces complexities in aligning diverse local priorities and managing inter-jurisdictional collaboration [73]. National governance plays a pivotal role in setting overarching resilience policies and frameworks that guide regional and local efforts. National-level decisions can significantly influence the allocation of resources, the establishment of regulatory standards, and the prioritization of resilience initiatives. However, the implementation timelines at this scale may be extended due to bureaucratic processes and the need for consensus among various stakeholders [74], while the core of organization may have operational issues in translating all the levels in good practices of resilience. In complex operational environment, it is essential that the assessment of "soft functions" consider multi-scalar complexities and possible conflicts between stakeholders defining also if these very same dynamics can represent single point of failures for the network43. The use of stress testing and tabletop exercises can approach this challenging element by using facilitating questions targeted to technological interdependencies but also human interdependencies [75,76]. In this case, it would be expected that outcomes from the risk agnostic approach are more directly associated with the lack of baselines needed for capacity maintenance e.g. best practices and codes of conduct, or blind spots in the allocation of responsibility internal or external to the organizations that are part of the stakeholder group. This approach could highlight resource inefficiencies, assuring that the baseline capacity is fully understood, used, and its possible gaps are addressed.

Governance and management of these resilience archetypes for infrastructure systems is subject for strategic and intervention-based decision-making [77–81]. Pertinent decision-making processes should be agile and responsive, able to quickly detect and respond to the changing conditions, while balancing the trade-offs between the short-term and long-term objectives. However, the presence of multiple stakeholders with competing priorities may impact the framework's effectiveness. A more detailed discussion on how the framework accommodates these multi-scalar complexities and stakeholder interactions, possibly within the Behavioral Changes section, would enhance its practical utility.

Despite its potential benefits, significant challenges remain in fully implementing the threat-agnostic approach to infrastructure resilience [82–85]. Moving towards network principles requires substantial investments in the sensing, collection, integration and cleaning of data that is not universally available. This challenge is compounded by the complex, interdependent nature of modern infrastructure systems, which makes isolating and measuring the impact of individual resilience characteristics as well as their systemic corollaries difficult [86,87]. However, investments towards threat agnostic resilience analysis are a necessity due to the exposure of complex infrastructure to ahistorical climatological and environmental stressors, a burgeoning global population, increasingly complex and interdependent economic activities, and the increasing disruptive potential for cyber and digital shock. Much needs to be done to better understand and translate the dimension of threat agnosticism and its implications across various spheres. This includes the organizational sphere, the social and behavioral sphere, and the political and governance sphere, all of which are often characterized by silo thinking in both theory and practice.

Implementing, tracking, and controlling threat-agnostic resilience within infrastructural systems requires deeper analysis based on the metrics for each resilience principle that this paper recommends. Governors, practitioners, and researchers alike may question the

most favorable composition of any infrastructure system based on its setting. Moreover, balancing these characteristics together will require an individualized approach for any infrastructure system. Further research should uncover the steps necessary within stress-testing these resilience characteristics to determine the most practical, cost-effective resilience characteristics within individual and interconnected systems.

CRediT authorship contribution statement

Benjamin D. Trump: Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization. **Stergios-Aristoteles Mitoulis:** Writing – review & editing, Methodology, Conceptualization. **Sotirios Argyroudis:** Writing – original draft, Formal analysis. **Gregory Kiker:** Validation, Formal analysis, Conceptualization. **José Palma-Oliveira:** Writing – review & editing, Methodology, Formal analysis. **Robert Horton:** Writing – review & editing, Resources, Conceptualization. **Gianluca Pescaroli:** Writing – review & editing, Methodology, Formal analysis. **Elizaveta Pinigina:** Writing – review & editing, Writing – original draft, Methodology. **Joshua Trump:** Writing – original draft, Methodology, Formal analysis. **Igor Linkov:** Writing – review & editing, Project administration, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Jose Palma Oliveira reports financial support was provided by Horizon Europe. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

Any opinions expressed herein are of the authors alone, and should not be considered the opinion or practice of any institution. Prof Stergios-Aristoteles Mitoulis and Prof Sotirios Argyroudis received funding by the UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee [grant agreement No: EP/Y003586/1, EP/X037665/1]. This is the funding guarantee for the European Union HORIZON-MSCA-2021-SE-01 [grant agreement No: 101086413] ReCharged - Climate-aware Resilience for Sustainable Critical and interdependent Infrastructure Systems enhanced by emerging Digital Technologies.

Data availability

No data was used for the research described in the article.

References

[1] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Syst. Mag. 21 (2001) 11–25.
[2] J. Andersson, V. Grassi, R. Mirandola, A conceptual framework for resilience: fundamental definitions, strategies and metrics, Computing 103 (2021) 559–588.
[3] I. Linkov, et al., Resilience stress testing for critical infrastructure, Int. J. Disaster Risk Reduct. 82 (2022) 103323.
[4] S. Thacker, et al., Infrastructure for sustainable development, Nat. Sustain. 2 (2019) 324–331.
[5] M. De Iuliis, A. Cardoni, G.P. Cimellaro, Resilience and safety of civil engineering systems and communities: a bibliometric analysis for mapping the state-of-the-art, Saf. Sci. 174 (2024) 106470.
[6] M. Sathurshan, A. Saja, J. Thamboo, M. Haraguchi, S. Navaratnam, Resilience of critical infrastructure systems: a systematic literature review of measurement frameworks, Infrastructures 7 (2022) 67.
[7] Z. Yang, et al., Indicator-based resilience assessment for critical infrastructures-A review, Saf. Sci. 160 (2023) 106049.
[8] S.A. Mitoulis, et al., Conflict resilience framework for critical infrastructure peacebuilding, Sustain. Cities Soc. 104 (2023) 104405.
[9] I. Linkov, B.D. Trump, Resilience quantification and assessment, in: *The Science and Practice of Resilience* 81–101, Springer, 2019.
[10] B.D. Trump, et al., Social resilience and critical infrastructure systems, in: I. Linkov, J.M. Palma-Oliveira (Eds.), Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, Springer Netherlands, 2017, pp. 289–299.
[11] M. Korkali, et al., Reducing cascading failure risk by increasing infrastructure network interdependence, Sci. Rep. 7 (2017) 44499.
[12] A. Rahmani, M. Ji, M. Mesbahi, M. Egerstedt, Controllability of multi-agent systems from a graph-theoretic perspective, SIAM J. Control Optim. 48 (2009) 162–186.
[13] W.-J. Ma, J. Wang, V. Gupta, C. Chen, Distributed energy management for networked microgrids using online ADMM with regret, IEEE Trans. Smart Grid 9 (2018) 847–856.
[14] Y.Y. Liu, J.J. Slotine, A.L. Barabási, Controllability of complex networks, Nature 473 (2011) 167–173.
[15] X. Xu, et al., Transportation network redundancy: complementary measures and computational methods, Transp. Res. Part B Methodol. 114 (2018) 68–85.
[16] B.D. Youn, C. Hu, P. Wang, Resilience-driven system design of complex engineered systems, J. Mech. Des. 133 (2011) 101011.
[17] H. Yu, V. Anand, C. Qiao, G. Sun, Cost efficient design of survivable virtual infrastructure to recover from facility node failures, IEEE Int. Conf. Commun. 1–6 (2011).
[18] S. Mishra, T.F. Welch, M.K. Jha, Performance indicators for public transit connectivity in multi-modal transportation networks, Transp. Res. Part A Policy Pract. 46 (2012) 1066–1085.
[19] B. Nowell, C.P. Bodkin, D. Bayoumi, Redundancy as a strategy in disaster response systems: a pathway to resilience or a recipe for disaster? J. Contingencies Crisis Manag. 25 (2017) 123–135.
[20] E.J. Oughton, et al., Infrastructure as a complex adaptive system, Complexity 2018 (2018) 3427826.
[21] K.E. Weick, K.M. Sutcliffe, Managing the Unexpected: Resilient Performance in an Age of Uncertainty, John Wiley & Sons, 2011.
[22] P. del Río, M. Burguillo, Assessing the impact of renewable energy deployment on local sustainability: towards a theoretical framework, Renew. Sustain. Energy Rev. 12 (2008) 1325–1344.

[23] L.S. McNeill, M. Edwards, Iron pipe corrosion in distribution systems, J. AWWA 93 (2001) 88–100.
[24] J. Mora-Rodríguez, X. Delgado-Galván, H.M. Ramos, P.A. López-Jiménez, An overview of leaks and intrusion for different pipe materials and failures, Urban Water J. 11 (2014) 1–10.
[25] B. Walker, A.S. Crépin, M. Nyström, Response diversity as a sustainability strategy, Nat. Sustain. 6 (2023) 621–629.
[26] M.A. Mohamed, T. Chen, W. Su, T. Jin, Proactive resilience of power systems against natural disasters: a literature review, IEEE Access 7 (2019) 163778–163795.
[27] E.K. Morris, et al., Choosing and using diversity indices: insights for ecological applications from the German biodiversity exploratories, Ecol. Evol. 4 (2014) 3514–3529.
[28] K. Ivashchenko, et al., Assessing soil-like materials for ecosystem services provided by constructed technosols, Land 10 (2021) 11.
[29] S. Villéger, N.W.H. Mason, D. Mouillot, New multidimensional functional diversity indices for a multifaceted framework in functional ecology, Ecology 89 (2008) 2290–2301.
[30] R. Cantelmi, G. Di Gravio, R. Patriarca, Reviewing qualitative research approaches in the context of critical infrastructure resilience, Environ. Syst. Decis. 41 (2021) 341–376.
[31] Y. Yang, S.T. Ng, F.J. Xu, M. Skitmore, Towards sustainable and resilient high density cities through better integration of infrastructure networks, Sustain. Cities Soc. 42 (2018) 407–422.
[32] J.K. Watts, K.W. Koput, Supple networks: preferential attachment by diversity in nascent social graphs, Netw. Sci. 2 (2014) 303–325.
[33] B. Walker, C.S. Holling, S.R. Carpenter, A. Kinzig, Resilience, adaptability and transformability in social–ecological systems, Ecol. Soc. 9 (2004).
[34] E.J. Gilrein, et al., Concepts and practices for transforming infrastructure from rigid to adaptable, Sustain. Resil. Infrastruct. 6 (2021) 213–234.
[35] M. Cespedes, J. Sun, Adaptive control of grid-connected inverters based on online grid impedance measurements, IEEE Trans. Sustain. Energy 5 (2014) 516–523.
[36] A. Darvishan, G.J. Lim, Dynamic network flow optimization for real-time evacuation reroute planning under multiple road disruptions, Reliab. Eng. Syst. Saf. 214 (2021) 107644.
[37] H. Vajjarapu, A. Verma, Composite adaptability index to evaluate climate change adaptation policies for urban transport, Int. J. Disaster Risk Reduct. 58 (2021) 102205.
[38] K. Gumasta, S. Kumar Gupta, L. Benyoucef, M.K. Tiwari, Developing a reconfigurability index using multi-attribute utility theory, Int. J. Prod. Res. 49 (2011) 1669–1683.
[39] I. Linkov, et al., Enhancing resilience in Post-COVID societies: by design or by intervention? Environ. Sci. Technol. 55 (2021) 4202–4204.
[40] E. Mahoney, et al., Resilience-by-Design and resilience-by-intervention in supply chains for remote and Indigenous communities, Nat. Commun. 13 (2022) 1.
[41] D. Simchi-Levi, et al., Identifying risks and mitigating disruptions in the automotive supply chain, Interfaces 45 (2015) 375–390.
[42] CISA, National critical functions set. https://www.cisa.gov/national-critical-functions-set, 2022.
[43] G. Pescaroli, et al., Managing systemic risk in emergency management, organizational resilience and climate change adaptation, Disaster Prev. Manag. 32 (2023) 234–251.
[44] Pescaroli, G., McMillan, L., Gordon, M., Aydin, N.Y., Comes, T., Maraschini, M. & Linkov, I. Definitions and Taxonomy for High Impact Low Probability (Hilp) and Outlier Events. Available at SSRN 5113134.
[45] Á. Carmona-Cabrero, R. Muñoz-Carpena, W.S. Oh, R. Muneepeerakul, Decomposing variance decomposition for stochastic models: application to a proof-of-concept human migration agent-based model, J. Artif. Soc. Soc. Simul. 27 (2024) 16.
[46] C.S. Holling, Resilience and stability of ecological systems, Annu. Rev. Ecol. Syst. 4 (1973) 1–23.
[47] R. Hassan, A. Yosri, M. Ezzeldin, W. El-Dakhakhni, Robustness quantification of transit infrastructure under systemic risks: a hybrid network–analytics approach for resilience planning, J. Transp. Eng. Part A Syst. 148 (2022) 04022089.
[48] Y. Kim, Y.S. Chen, K. Linderman, Supply network disruption and resilience: a network structural perspective, J. Oper. Manag. 33 (2015) 43–59.
[49] G. Rapisardi, I. Kryven, A. Arenas, Percolation in networks with local homeostatic plasticity, Nat. Commun. 13 (2022) 122.
[50] T.P. Bostick, E.B. Connelly, J.H. Lambert, I. Linkov, Resilience science, policy and investment for civil infrastructure, Reliab. Eng. Syst. Saf. 175 (2018) 19–23.
[51] R. Sitzenfrei, et al., Impact of hybrid water supply on the centralised water system, Water 9 (2017) 855.
[52] L. Molyneaux, C. Brown, L. Wagner, J. Foster, Measuring resilience in energy systems: insights from a range of disciplines, Renew. Sustain. Energy Rev. 59 (2016) 1068–1079.
[53] D.J. Yu, et al., Toward general principles for resilience engineering, Risk Anal. 40 (2020) 1509–1537.
[54] M. Mashal, A. Palermo, G. Keats, Innovative metallic dissipaters for earthquake protection of structural and non-structural components, Soil Dyn. Earthq. Eng. 116 (2019) 31–42.
[55] Caltrans, I-210 Connected Corridors Pilot Project (2025). https://dot.ca.gov/caltrans-near-me/district-7/district-7-projects/d7-i210-corridor-pilot-project.
[56] A.A. Ganin, et al., Resilience and efficiency in transportation networks, Sci. Adv. 3 (2017) e1701079.
[57] M. Dutta, Organisational restructuring of Indian Railways, Case Stud. Transp. Policy 10 (2022) 66–80.
[58] P. Patlakas, et al., The eastern mediterranean extreme snowfall of January 2022: synoptic analysis and impact of sea-surface temperature, Weather 79 (2024) 25–33.
[59] C. Kakderi, E. Oikonomaki, I. Papadaki, Smart and resilient urban futures for sustainability in the post COVID-19 era: a review of policy responses on urban mobility, Sustainability 13 (2021) 6486.
[60] J.P. Montoya-Rincon, et al., A socio-technical approach for the assessment of critical infrastructure system vulnerability in extreme weather events, Nat. Energy 8 (2023) 1002–1012.
[61] L. Xing, Cascading failures in internet of things: review and perspectives on reliability and resilience, IEEE Internet Things J. 8 (2020) 44–64.
[62] R. Parshani, S.V. Buldyrev, S. Havlin, Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition, Phys. Rev. Lett. 105 (2010) 048701.
[63] M. Kivelä, et al., Multilayer networks, J. Complex Netw. 2 (2014) 203–271.
[64] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. Eng. Syst. Saf. 121 (2014) 43–60.
[65] R.R. Liu, et al., The “weak” interdependence of infrastructure systems produces mixed percolation transitions in multilayer networks, Sci. Rep. 8 (2018) 2111.
[66] R. Guidotti, et al., Modeling the resilience of critical infrastructure: the role of network dependencies, Sustain. Resil. Infrastruct. 1 (2016) 153–168.
[67] L. Fraccascia, I. Giannoccaro, V. Albino, Resilience of complex systems: state of the art and directions for future research, Complexity 2018 (2018) 3421529.
[68] S.A. Argyroudis, et al., Digital technologies can enhance climate resilience of critical infrastructure, Clim. Risk Manag. 35 (2022) 100387.
[69] D.E. Alexander, Confronting Catastrophe: New Perspectives on Natural Disasters, Terra Publishing, 2000.
[70] G. Pescaroli, D. Alexander, Critical infrastructure, panarchies and the vulnerability paths of cascading disasters, Nat. Hazards 82 (2016) 175–192.
[71] A. Boin, M.J.G. van Eeten, The resilient organization, Public Manag. Rev. 15 (2013) 429–445.
[72] K. Kok, T. Veldkamp, Scale and governance: conceptual considerations and practical implications, Ecol. Soc. 16 (2011) 23.
[73] A. Abdillah, I. Widianingsih, R.A. Buchari, H. Nurasa, Resilience-based governance: a public administration perspective and resilience agenda, Public Organ. Rev. (2025), https://doi.org/10.1007/s11115-025-00834-z.
[74] A. Boin, F. Bynander, E. Stern, P. t Hart, Leading in a Crisis: Organisational Resilience in Mega-Crises, ANZSOG, 2020.
[75] R. Horton, B.D. Trump, J. Trump, H.S. Knowles, I. Linkov, P. Jones, G. Kiker, Performance metrics for resilience of airport infrastructure, Transp. Res. Part D Transp. Environ. 104676 (2025).
[76] R. Horton, G.A. Kiker, B.D. Trump, I. Linkov, International airports as agents of resilience, J. Contingencies Crisis Manag. 30 (2022) 217–221.
[77] M. Chester, et al., Infrastructure resilience to navigate increasingly uncertain and complex conditions in the anthropocene, NPJ Urban Sustain. 1 (2021) 4.
[78] E.M. Wells, et al., Modeling critical infrastructure resilience under compounding threats: a systematic literature review, Prog. Disaster Sci. 15 (2022) 100244.
[79] CISA, Methodology for Assessing Regional Infrastructure Resilience—Lessons Learned from the Regional Resiliency Assessment Program June 2021, 2021.

[80] S.V. Buldyrev, et al., Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[81] J. Lawrence, P. Blackett, N.A. Cradock-Henry, Cascading climate change impacts and implications, Clim. Risk Manag. 29 (2020) 100234.
[82] M.V. Chester, B. Allenby, Infrastructure as a wicked complex process, Elem. Sci. Anth. 7 (2019) 21.
[83] J.J. Magoua, N. Li, The human factor in the disaster resilience modeling of critical infrastructure systems, Reliab. Eng. Syst. Saf. 232 (2023) 109073.
[84] The White House, National Climate Resilience Framework, 2023.
[85] M.M. Danziger, A.L. Barabási, Recovery coupling in multilayer networks, Nat. Commun. 13 (2022) 955.
[86] Andrew S. Jin, et al., Building resilience will require compromise on efficiency, Nat. Energy 6 (11) (2021) 997–999.
[87] IRGC, Guidelines for the governance of systemic risks, International Risk Governance Center: Lausanne (2018), https://doi.org/10.5075/epfl-irgc-257279. https://infoscience.epfl.ch/server/api/core/bitstreams/74f26a3b-a269-4afd-96e4-ec0ab6dc79a3/content.