1 Introduction

The concept of critical infrastructure resilience has been attracting considerable interest, particularly after several notable natural disasters that affected some of the most developed economies in the world. Examples of these natural disasters include Hurricane Katrina in 2005 and Superstorm Sandy in 2012, both of which affected the United States, and the 2011 earthquake and tsunami that affected Japan. The increased interest that the topic of critical infrastructure resilience is attracting in academia, government, commerce, services, and industry is creating an alternative engineering field that could be called resilience engineering. However, the views of the meaning of resilience have varied, and even in some very relevant world languages an exact translation of the word "resilience" either has only recently been introduced – for example, the word "*resiliencia*" was added to the dictionary of the Royal Academy of Spanish Language in 2014 – or it still does not exist, as in Japanese. Thus, this chapter introduces the main concepts associated to the study of resilience engineering applicable to critical infrastructure systems with a focus on electric power grids and information and communication networks (ICNs) because these are the infrastructures that are identified as "uniquely critical" in the US Presidential Policy Directive 21, which is the source for the definition of resilience that is used in this book.

1.1 Historic Review of the Concept of Infrastructure Resilience

The Merriam-Webster dictionary defines resilience as the "capability of a strained body to recover its size and shape after deformation caused especially by compressive stress," and the "ability to recover from or adjust easily to misfortune or change" [1]. This source also indicates that resilience originates in the Latin verb *resilire* which means "to jump back or to recoil." That is, the conventional definition of resilience refers to the capability of recovering from an adverse condition, so more resilient systems tend to show a more elastic behavior to a given stressful action. This definition is the basis for the original reference to resilience in science and engineering in which resilience of a material is defined as "the ability of a material to absorb energy when it is deformed elastically, and release that energy upon unloading" [2]. That is, the more a material can absorb energy by deforming elastically – thus, being able to return to the original state once the energy is released back – the more resilient the material is.

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

Similar definitions can be found in other material sciences contemporary works [3] and in publications for civil engineers dating more than a hundred years ago [4]. Mathematically, the concept of resilience originates in Hooke's law, which indicates that while a material is showing a resilient behavior there is a linear relationship between the stress or force applied to the material and the strain or deformation observed in the material. If the material is deformed beyond point A in Fig. 1.1, then some deformation will be permanent and the relationship between stress and strain will no longer be linear. If the material continues to be deformed up to point B in Fig. 1.1, then it will fracture. Resilience, in this context, is measured based on the modulus of resilience equal to the area under the stress–strain curve up to point A in Fig. 1.1.

The concept of resilience related to the elasticity of materials represented by Hooke's law is one of the basic notions in structural engineering. Hence, civil engineers have been applying this concept of resilience as part of their studies when designing all types of structures and in particular when aiming at improving the performance of buildings, bridges, and other structures during earthquakes or other extreme events, such as high winds. Hence, civil engineering has been one of the main fields that have traditionally applied the notion of resilience for a considerable time. However, it is important to recognize that this concept of resilience associated to the elasticity of materials is only loosely related to the notion of resilience that is currently considered for critical infrastructures and that will be discussed in detail in the next section of this chapter. Recovery speed is the closest notion in such a definition of resilience that relates to elasticity. However, the definition of resilience from materials sciences provides no indication about how long it will take for a material under stress to return to the original state. It just indicates that once the stress is removed, the material will be able to return to its original state provided that the resilient limit is not exceeded. Nevertheless, the deformation theory of materials also identifies some other concepts often related to that of resilience. In particular, in materials science *toughness* is the "ability of a material to absorb energy without fracturing" [3].

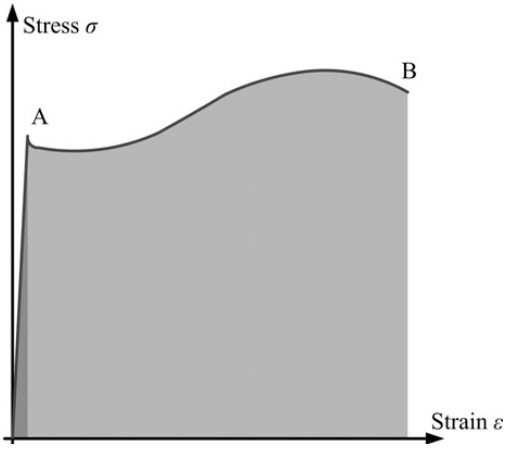

Figure 1.1 Stress–strain curve of a steel bar when being stretched.

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

Toughness is measured based on the modulus of toughness, which equals the area under the stress–strain curve in Fig. 1.1 up to point B.

Eventually, the concept of resilience was applied in other contexts and fields of study. As [5] indicates, in the early 1970s a concept of resilience was applied to ecology; but more importantly than the fact that resilience was applied to other fields different from materials science is that, as is also pointed out in [5], the original concept of resilience has been seen since then as limited and in need of adjustment in order to be able to describe the notions that need to be represented in contexts different from the traditional one in materials science and structural engineering. In [5] resilience is applied within the context of one of the other main fields that originated the present definition of resilience applicable to critical infrastructures: risk analysis. One of the common attributes associated to resilience in both ecology and risk analysis is the concept of adaptation. More recently, the concept of adaptation has been associated to changes in systems, organizations, or organisms due to stresses related to climate change [6]–[7], but originally these stresses have been related to unexpected events [5]. Another work that recognizes the need to broaden the definition of resilience in order to include adaptation as an attribute of resilience in the context of risk and safety analyses is [8]. But [8] also makes an important observation that is key in understanding the historical evolution of the definition of resilience. In [8] the notion of operational resilience is described as "the ability of a system to adapt its behavior to maintain continuity of function (or operations) in the presence of disruptions." In this definition, the concept of adaptation is different from the concept of adaptation used in the next section of this chapter because here adaptation refers to a short-term temporary adjustment during disruptions, whereas adaptation in the context of the resilience definition used throughout this book and explained in the next section refers to long-term and permanent changes that do not necessarily occur while the disruptions are present. However, [8] seems to be the first work to explicitly recognize the need for including how infrastructure systems are operated as a factor influencing resilience. Such inclusion of infrastructure operations as a factor affecting resilience broadened the idea of resilience and allowed it to evolve from a concept based on structural characteristic of system components within the almost exclusive realm of materials science and civil engineering into a more holistic idea that requires a multidisciplinary perspective for its thorough study.

Once the idea of infrastructure operations is considered to be a relevant factor influencing resilience, it is then possible to identify other factors that affect resilience and modifies its concept beyond the idea of elasticity originated in materials science. One of these other factors, identified in [9], relates to human influence and actions in not only the direct operation of infrastructures but also their participation in the creation and management of organizations – namely companies, cooperatives, and so on – that form the skeleton used to operate such infrastructures. Such organizations are managed based on processes, procedures, legal and financial documents, and other written and nonwritten management instruments that have a direct influence on infrastructure performance during extreme events. For example, employee training programs have a direct influence on how lessons from a past disaster can be transmitted

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

so that changes can be implemented as part of an adaptation process to improve resilience. But these lessons will not be learned without a formal and systematic process that studies the effects of extreme events on infrastructures. Such a process should be developed based on the notions applied in disaster forensics [10]–[11], which is a part of the resilience engineering field that is discussed in detail in Chapter 5. Hence, implementation of a disaster forensics process has a direct influence on the adaptation capabilities of an organization. Another example of human-driven processes affecting resilience is how the implementation of logistical, human, and physical resources management processes affects service restoration time after a disaster, which, as discussed, constitutes another of the factors that are part of the broader view of resilience.

The concept of resilience has also been applied to electric power grids for a considerable time. However, the traditional concept of resilience applied to electric power grids was limited to the idea of quick recovery after an extreme event. Such a view is found in works like [12] that defines resilience as "the ability of a system to bounce back from a failure." A similar definition of resilience aspects is discussed in [13], which defines resilience as "the ability of a system to respond and recover from an event." A similar definition is assumed when it is suggested to measure resilience based on the "trajectory of a recovery time following a catastrophic event" [14]. However, such a definition of resilience provides an incomplete description of what resilience means. Even when considering the original definition of resilience from materials science, such a definition is based on the maximum deformation that can be observed within an elastic behavior and not a given deformation observed for a particular test. That is, defining resilience based only on recovery speed neglects the fact that, as indicated, recovery times are influenced by human-based organizational processes, such as logistic and resource management and personnel training, that relate to adaptation capabilities [15]. Moreover, another important fact being neglected is that a more damaged infrastructure will likely take longer to recover than a less damaged infrastructure. That is, when defining resilience within the context of infrastructure systems, it is also important to include how well such a system is able to withstand the disruptive effects of the extreme event under consideration. Likewise, a more prepared infrastructure operator (with necessary spare resources, contracts in place, a plan of action to conduct service restoration, etc.) will have shorter recovery times than a less prepared infrastructure operator. Hence preparation and planning activities in order to make the infrastructure system able to withstand the extreme event disruptions better and to shorten the service restoration time need also be considered as part of a definition of resilience.

The concept of resilience is also sometimes seen as historically related to reliability [16]–[17]. However, although it is possible to find analogies in some ideas and concepts in resilience and in reliability studies, there are significant differences between these two fields. The main difference between these two fields is that while the broad field of reliability and availability is applicable to the performance of systems and their components under what is considered normal operating conditions over long periods of times when there are ideally an infinite number of failure and repair cycles,

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

resilience in the context of critical infrastructures applies to the performance of systems and their components with respect to extreme events that have a low probability of happening. Thus, if extreme events are observed, they happen a very small number of times during the expected life of a system.

Although the concept of reliability for electric power distribution grids is not applied in a strict sense with respect to the formal definition of reliability applicable to industrial components [18], it is still possible to observe differences between the use of the terms resilience and reliability. Such a distinction is demonstrated by the fact that the IEEE Standard 1366 [19] about electric power distribution reliability indexes explicitly excludes "major event days" (i.e., days under the effect of natural disasters) from these reliability calculations; that is, reliability indexes are calculated under "normal conditions." However, in the electric power industry as a whole there has not been a consistent differentiation in the use of both terms. This lack of consistency has led to considerable confusion in the use of both terms applicable to electric power grids. Such confusion may have been in part originated by the North American Electric Reliability Corporation (NERC), when in its Severe Impact Resilience Task Force report of May 2012 [16] it measured resilience with respect to reliability levels. While, as indicated, the traditional understanding of the term resilience in power grids relates to service restoration capability after a disruption, one of the main definitions for reliability is "the ability of the bulk power system to withstand sudden disturbances, such as electricity short circuits or unanticipated loss of system elements from credible contingencies, while avoiding uncontrolled cascading blackouts or damage to equipment" [20]. However, in [17] resilience was defined as "the ability to withstand grid stress events without suffering operational compromise or to adapt to the strain so as to minimize compromise via graceful degradation." Hence it is clear that there has been considerable confusion within the electric power industry between the concepts of reliability and resilience. While the next section describes the concept of resilience applied throughout this book, it can be emphasized that a main difference between a resilience and a reliability assessment is that the former applies to relatively uncommon events, whereas the latter applies to "normal" operating conditions.

Some degree of confusion has also existed, particularly for power grids, between the concepts of security and resilience. This confusion may have originated in part because, before 2001, NERC used the term security instead of the term reliability indicated earlier [21], which was then followed in [16] by using reliability as a measure of resilience. The relationship between security and reliability in power grids can be clearly observed when in [16] relay security is defined as "the degree of certainty that a relay or relay system will not operate incorrectly," which can be interpreted as the relay reliability from conventional reliability theory from industrial components. Traditionally, the concept of power grid security includes three functions: system monitoring, contingency analysis, and security-constrained power flows [22]. These three functions relate to the analysis of contingencies (e.g., faults) and outages under normal operating conditions. However, this concept of security started to be confused with that of cybersecurity once this latter term became more popular as smart grid technologies started to be developed in the

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

Figure 1.2 Remains of a building in Mexico City after the September 2017 earthquake. The painting on the wall reads "Juan ♥ resilencia." (Note from the author: the correct spelling for this term in Spanish is resiliencia. This mistake was probably due to the fact that resiliencia is a new term in Spanish.)

early 2000s. Hence in this book the traditional understanding of the concept of security applicable to power grids is not applied. Instead, discussion about security is related to the protection of necessary material or human resources from harm. Likewise, in this book the related concept of cybersecurity is applied within the context of the protection of control and sensing subsystems of a power grid or of data in a critical infrastructure system. Moreover, throughout this book the concept of reliability is considered to be based on the traditional definition applicable to industrial components in which reliability of an "entity is the probability that this item will operate under specified conditions without failure from some initial time $t = 0$ when it is placed into operation until a time t" [18].

Nowadays, resilience has evolved into a broader techno-social concept related to community resilience that has common elements to the notion of resilience applicable to critical infrastructure systems, such as the need for adaptation and preparation for a disruptive event. Such a relationship originated in the fact that societies as a whole and people at an individual level have grown increasingly dependent on critical infrastructure systems and in particular on electric power and communications, as explicitly acknowledged in [23]. As demonstrated by Fig. 1.2, such a concept has also been increasingly accepted by people, even in areas with languages in which such a term did not exist before. However, because of the various interpretations that the concept of resilience and the different contexts in which it is used, the next section discusses the definition of resilience used in this book within the context of critical infrastructure systems.

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

1.2 Definitions of Resilience

The previous section has shown that understanding resilience within the context of critical infrastructure systems involves four main attributes:

- Capacity for a rapid recovery when a disruption happens.
- Ability to adapt in order to improve resilience to disruptive events.
- Capability to withstand the disruptive actions of the extreme event.
- Competency for planning and preparing for the disruptive event.

Hence, in this work, resilience is defined based on [23] as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions." This definition is similar to the one adopted by different countries [24] and institutions [25]. One of the implicit consequences of considering this definition is that the idea of resilience is no longer about a concept applicable only during an event or test, as it is applicable when testing a material's elastic characteristics. As Fig. 1.3 shows, a disruptive or extreme event can be considered to have multiple phases. The initial phase is when the extreme event happens. It is during this phase, which may last from a few minutes to a few days, that the disruptive effects of the event act on the infrastructure system. Thus, the withstanding capability is particularly important during this initial phase of the event. Activities during this phase are focused on survival and targeted response. The immediate aftermath is the phase that follows immediately after the disruptive event has concluded. This phase typically lasts from a few days to a few weeks. During the immediate aftermath, infrastructure elements that were affected during the extreme event are repaired or reconstructed and service restoration takes place. Activities during this phase also include evaluation of system status through field assessments. Hence the recovery process mostly takes place during the immediate aftermath. Once repairs (either temporary or permanent) are mostly completed, the intermediate aftermath phase starts, which may last from a few weeks to several months. In this phase, lessons from the extreme event are learned by, for

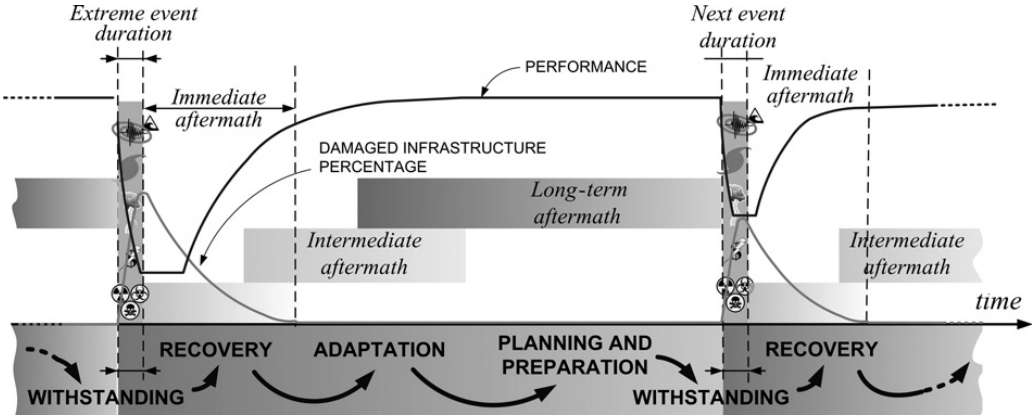

Figure 1.3 Extreme event phases and related resilience attributes.

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

example, performing forensic analyses. This learning process is an essential component of the adaptation mechanism that is then applied in the next phase when the changes needed to improve resilience for the next event are planned. The phase that follows the intermediate aftermath is the long-term aftermath, which may last from a few months to several years. The activities focus on preparing for the next event through planning and mitigation. During this phase, infrastructures may be modified in order to make them more resilient for a possible next event or to adapt to lingering effects of the previous event, such as economic effects of a reduced load in power grids. Such infrastructure modifications are made without certainty concerning if or where and when the next disruptive event will happen. Such uncertainty involves a cost associated with the preparation decisions, which are usually assessed and evaluated using risk analysis techniques.

The discussion in the previous paragraph indicates that the concept of resilience is applicable to multiple timescales, with some attributes applicable at short timescales while others are applicable at longer timescales. Although some works [26]–[27] have presented a sequential phase process in which the adaptation and preparation for the next event are considered a feedback learning loop, such a description could be argued to neglect the fact that, as indicated, planning and preparation activities are performed without having the certainty that a next event will happen or when or where it will happen. This is a fundamental conditioning aspect of the planning process. As a result of an unknown future or lack of certainty about it, the preparation and adaptation process is better described as a feed-forward process that looks ahead while making decisions based on the input provided by the lessons of the past. Otherwise, considering the adaptation and preparation process as feedback may be considered to be a violation of causality rules that are part of any time-dependent process. A typical example of the limitations of preparing for an uncertain future can be found in the common suggestion of having most or all of the overhead electric power infrastructure placed underground in order to make it more resistant to storms and to address other issues [28]. However, the cost of laying power lines underground is significant, so such an investment is of very difficult practical implementation and, if done, there is always a possibility that the storm that would make such investment worthwhile would never happen during the lifetime of such underground infrastructure components. One alternative could be to do such infrastructure modifications in particular areas but, as indicated, even if there are high chances of a disruptive storm happening within a given time period, the area that such a storm would affect is unknown (as happens with tornadoes) or the area could be too large (e.g., with hurricanes) to make the localized solutions effective. Finally, it is worth mentioning that such a solution intended to make power grids more resistant to storms may not necessarily make them more resilient, because repairing damaged buried infrastructure takes more time than reconstructing damaged overhead cabling systems. Thus, although the withstanding capabilities against storms of a buried infrastructure could be improved, its recovery speed may worsen. Furthermore, since faults in buried power infrastructure are more difficult to repair – thus, leading to longer power outages – than in overhead lines, system reliability understood in the traditional notion applicable to power grids – namely,

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

under "normal" operating conditions – will worsen even if the anticipated future storm that motivated the modifications from overhead to underground infrastructure never actually happens.

The notion of resilience applicable to infrastructure systems as a multitimescale concept yields additional consequences from those discussed earlier. One important concern in the aftermath of a disaster and explicitly acknowledged in [23] when it identifies energy and communications infrastructures as specially critical "due to the enabling functions they provide across all critical infrastructure sectors" is the effect that a loss of service of one infrastructure has on another infrastructure. This issue is particularly observed in the immediate aftermath of a disruptive event. A common example of such effects is observed with potable water distribution systems depending on electric power provided by a local utility grid for operating pumps. As discussed in more detail in Chapter 10, such a situation was particularly critical in the aftermath of Hurricane Maria when many communities in Puerto Rico could not receive water because the pumps were not operational during the long power outage that affected the island after the storm. Hence even when an infrastructure is undamaged, thus physically withstanding the event well, it may lose service because of the functional dependencies on services provided by another infrastructure, called a lifeline. Thus the resilience of a dependent infrastructure – the infrastructure system needing certain services provided by lifelines for its operation – may be affected by the resilience of its lifelines. Such dependence must be reflected in resilience metrics as discussed in Chapter 3.

In the intermediate and long-term aftermath, other types of dependencies affect critical infrastructure resilience. However, such dependence is more prevalent with respect to social services needed in order to support adaptation and preparation resilience components. Important examples of such social services include education and economic and financial services. Education services are key to supporting the learning process related to adaptation and, in particular, to reducing the effects of an aging workforce, which is considered to be one of the main vulnerabilities of electric power companies, as an increased number of employees are expected to retire. Economic and financial services dependence are critical not only during normal condition operations but particularly in the aftermath of disruptive events. Examples of such cases include the bankruptcies by Tokyo Electric Power Company (TEPCO) and Pacific Gas and Electric (PG&E); for the former, due to economic liabilities associated with the Fukushima #1 nuclear power plant disaster in the aftermath of the 2011 earthquake and tsunami in Japan, and for the latter, due to the 2018 wildfires in California. Another example can be found in Puerto Rico, where a long-lasting economic crisis, which eventually contributed to the Puerto Rico Electric Power Authority (PREPA) bankruptcy in 2017, significantly hindered preparation and mitigation activities for a potential future extreme event. These limitations were an important contributing factor for the extremely long power outage that followed Hurricane Maria when it hit the island at the end of September 2017. The multiple ways in which service dependencies affect resilience of critical infrastructure systems suggest that such systems are far more complex than an organized collection of

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

physical components. A more complex model for physical infrastructure, presented in [9] and [29] and also found in [30], represents these infrastructures as a combination of three domains as shown in Fig. 1.4:

- 1) a physical domain made up of the physical components necessary to deliver the services provided by the infrastructure system,
- 2) a human/organizational domain made up of the processes, policies, procedures, regulations, as well as the human system operators and administrators necessary to manage, administrate, and operate the infrastructure system, and
- 3) a cyber domain made up of databases, information, communications, and control and operations algorithms.

As also explained in [9] and [29], this model applies to all community systems, which include infrastructure and social systems. Social systems are "specific combinations of resources and processes developed to deliver services primarily through human interactions" [29]. Infrastructure systems "are specific combinations of resources and processes developed to deliver services primarily through a physical built environment or a cyber sub-system" [29]. In this context critical infrastructures are then defined, based on [24], as "the systems . . . that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations."

In turn, services are supported by resources. These resources are inputs used by the systems in order to provide services. For example, in an electric power grid, resources include poles, transformers, and other materials, and the labor force employed to operate the system and monetary assets used to procure fuel or pay employee salaries. These resources are typically part of services provided by other systems. For example, work force education and qualification is a service provided to community systems by an educational system. All domains of a community system interact with the community's physical and social environment, for example, when the weather affects operation of components in the physical domain or when information affects decisions people make in the human domain.

Disruptive events or extreme events could originate in the community environment or from within a community system. Typically, extreme events that originate in the community environment are natural disasters, whereas disruptive events that originate in community systems, such as an economic crisis impacting financing or revenue streams for utilities, are human-caused disasters. Disruptive events can be distinguished in other ways. Some events, such as tornadoes, are localized, while others, like earthquakes or hurricanes, affect large areas. Some events, like hurricanes, can be predicted with a relatively high degree of accuracy even days in advance, allowing for preparation activities to mitigate their impact; but other events, like earthquakes, although they can be anticipated, pose much greater uncertainties on when and where they will occur than the former type of events. Some events, like earthquakes and tornadoes, tend to occur very rapidly (within a matter of minutes), whereas other disruptive events, like droughts, occur on timescales of months or even years.

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

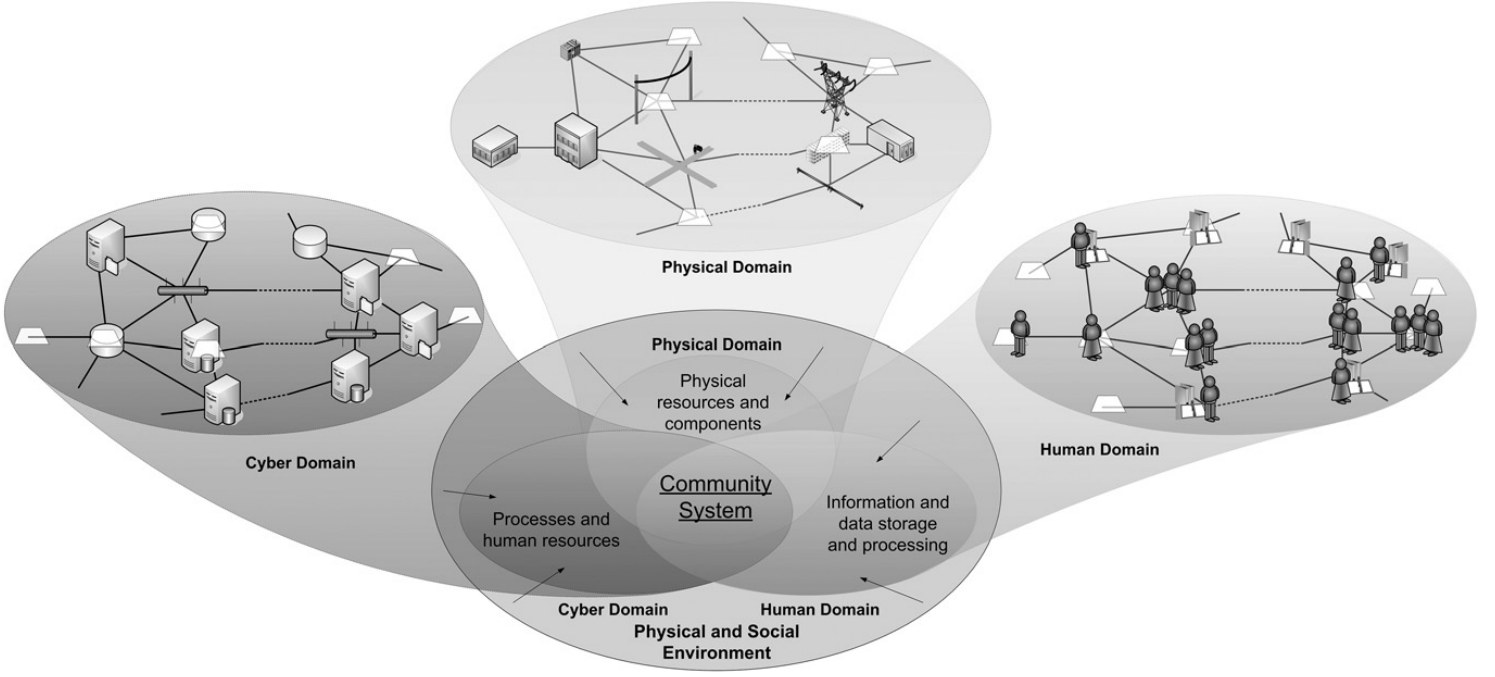

Figure 1.4 Graphical model of a community system showing its three domains.

In the model depicted in Fig. 1.4, which was presented in [9], each domain is modeled as a graph and thus each domain is made of vertices and edges. Each node or vertex represents a component or group of components necessary to provide a service. The connections or edges between vertices represent the provision of a given service. In the physical domain typically both edges and vertices may be related to physical elements. For example, the service "electric power provision" can be provided by an electric power grid, which in its physical domain is composed of vertices represented by network nodes, such as substations and power plants. These nodes are connected with electric power lines that are the physical realization of the service electric power provision between nodes. In other domains, it is possible for most cases to associate a vertex to a physical element, such as people or groups of people in the human domain or paper documents or data storage or processing equipment in the cyber domain. However, since edges represent service provision from one vertex to another, it may not be possible in general to associate an edge to a real piece of equipment or to people. Each service provision edge is characterized by specific attributes, such as a metric for quality of service. Vertices are also characterized based on given attributes in relationship with the function they provide within the community system, the domain they belong to, and how they are formed. Such attributes and the intended functions served by each vertex may establish a hierarchy of vertices. For example, in the human domain, vertices may be formed by a person or a group of people with certain skills working as a team with a given purpose. The service provided by some people (i.e., vertices in the human domain) could be to authorize the execution of processes or to administrate resources. Hence, these vertices may be at a higher hierarchy position than other vertices that may be dependent on the services provided by vertices at a higher hierarchical position in order to deliver their services adequately. Each domain graph has a dynamic structure with vertices and edges continuously being added or removed or with their attributes changing.

Vertices belong to the graph associated to a given service and can be classified into sink vertices, source vertices and passing vertices. The receiving end of a service is represented by a sink vertex. For example, a sink vertex could represent an electrical load in an electric grid power system. Source vertices represent the providing end of a service. The originating end of a service is a source vertex, which transforms services and resources into the originated service. Attributes of source vertices include what services they require as inputs, the transformation occurring so that input services and resources produce an output service, the type and characteristics of the output service, and possibly attributes of its service buffer (e.g., capacity). In passing, transfer, or transmission vertices, an input service is passed or transferred to other vertices without changing the service being provided. A transfer vertex without buffers could also be considered a back-to-back sink and source vertex without services transformation occurring in the latter; because the input and output services of a transfer vertex are the same, the function representing the transformation at the source end of the transfer vertex would not necessarily equal the neutral element associated with the considered service. The reason for these characteristics is that a transfer vertex may still require the provision of an input service different from the one being modeled in the graph

containing such a vertex in order for the transfer vertex to transfer the service modeled in the graph. For example, a substation could represent a vertex in the physical domain graph representing the electric power provision service. This substation typically will not require another input service in order to transfer the electric power provision service from its input to its outputs. However, a communications transmission site modeled as a vertex in the physical domain graph representing data transmission services typically requires the provision of electric power so data can be transmitted from the vertex's input to its output.

Since vertices typically require services provided by other vertices in order to, in turn, provide a service, it is possible to identify the existence of intradependencies within the community system, when those needed services are provided by the system to which the vertex belongs. These domain intradependencies are established due to the need of services by vertices in order to perform their intended function. Provision of services and establishment of intradependencies are observed within a domain or between domains of a community system. For example, administrative areas that are part of the human domain of an infrastructure system provide procurement services necessary to acquire physical components necessary for nodes in the physical domain so they can in turn provide their services. In other cases, services needed for a vertex are provided by another system. This service provision is the way community systems interact among themselves. These services are represented in Fig. 1.5 by arrows linking two of the community systems. Service provision between community systems is also characterized by attributes, such as quality of service and beginning and ending vertices. The need of community systems for services in order to provide their own services creates functional dependencies of a community system on services. That is, dependencies are established with respect to services. In some cases, a service either can be provided by another community system or could be provided internally, such as a wireless communications base station, which can be powered by an electric grid or by a local power plant using photovoltaic cells. Communication networks that are part of electric power grids and that are used for control and monitoring of such power grids is another example of needed services provided internally within a community system providing another service. However, in other cases, such as that of financing or commerce, services can only be provided by a single system, which cannot be replaced by services provided through alternative means internal within such a system. In these cases, it is possible to identify a lifeline, which, as indicated, is the community system provided the needed service, and a dependent community system, which is the one needing such a service in order to function.

When the need of a service from another community system is observed in a reciprocal way, then such interactions are called interdependencies. For example, Fig. 1.5 exemplifies such integrated interdependence of physical and social systems through physical, cyber, and social domains by representing some relevant services of interest. As indicated, power grid operating companies need economic and social services for their operation. Such service provision is indicated as (1) in Fig. 1.5. In turn, financial facilities (i.e., part of the physical domain of the economic and financial system) that are part of the resources used to support the provision of such financial

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

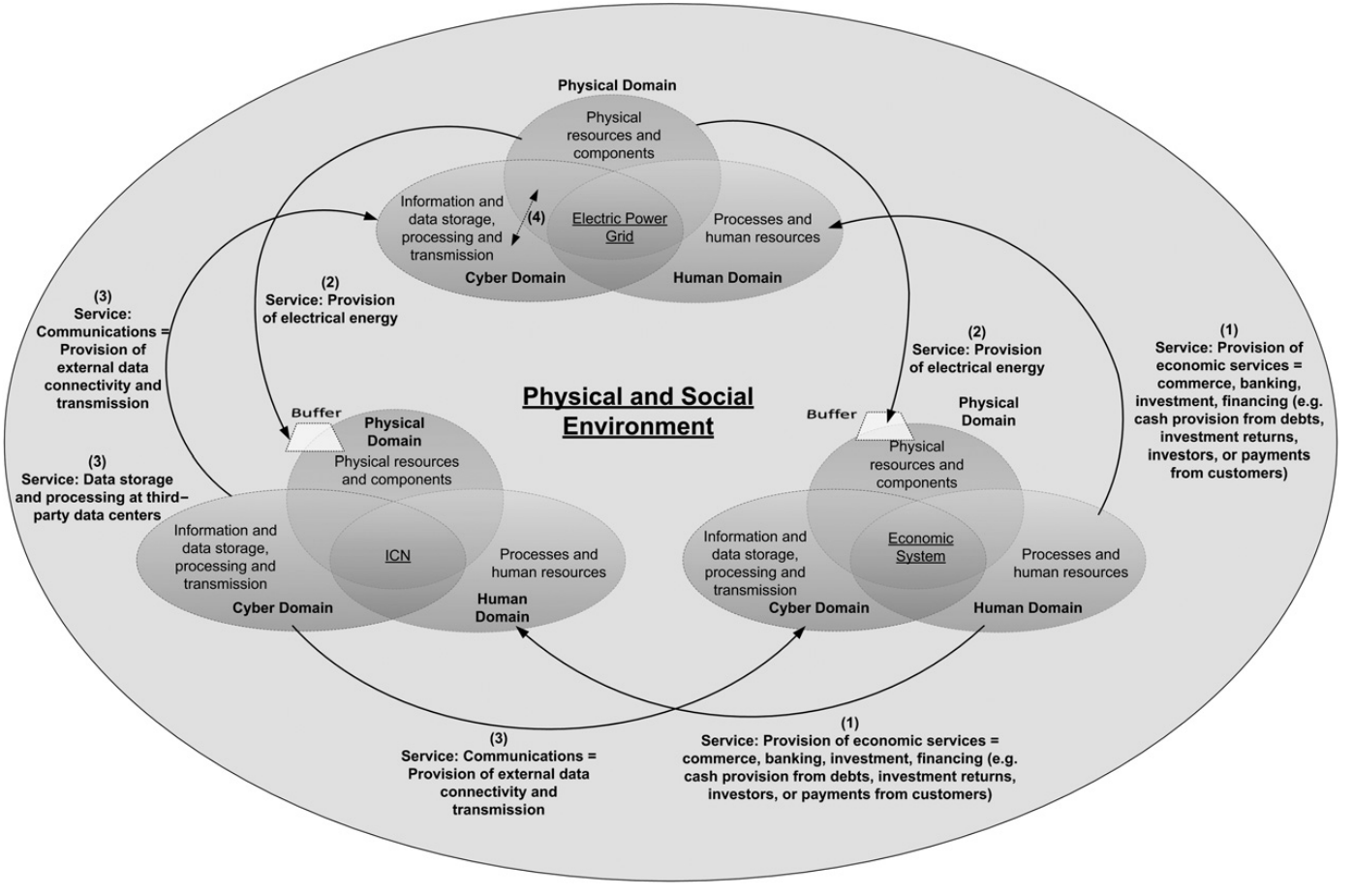

Figure 1.5 Service interactions among community systems establishing interdependencies.

services need electric power, which is almost always provided primarily from an electric grid. Electrical energy provision is thus represented by (2) in Fig. 1.5. One of the uses of such electrical energy is to power computers and other electronic resources supporting electronic financial transactions, which in developed countries is the primary means to conduct financial and economic functions. Such economic and financial data is, then, part of the cyber domain of the economic and financial system. Transmission of such data needs the corresponding service provided by an information and communications network, which is the third community system represented in Fig. 1.5, which also shows the provision of such data transmission service by (3). Additional services provided by an ICN may also include processing and storing such data in data centers. In turn, ICNs need electric power to operate the communications equipment. Such service is often primarily provided by an electric power grid, so (2) also depicts the provision of such service for ICNs as was indicated earlier for the economic system. Since there is a reciprocal dependence on services between electric power grids and ICNs, an interdependency is also established among these systems. It is possible to identify other services in addition to those shown in Fig. 1.5 and also apply these concepts to other community systems, but, for simplicity and clarity in the discussion, only those services and systems are the ones discussed here. Notice, however, that the communication services needed by power grids for system operation and control are not represented as a case of interdependence. Since communication services necessary for the operation of a power grid are most commonly provided by communications equipment belonging to the electric power grid assets and forming a private network, as exemplified by Fig. 1.6 and indicated in Fig. 1.5 by the service labeled as (4), they do not establish an interdependence. Instead, they establish an intradependence.

In addition to functional dependencies, interdependencies, and intradependencies, it is possible to identify other types of dependencies. These other types of dependencies include physical dependencies, such as the case when one infrastructure system uses physical resources of another infrastructure system to provide its services, and conditional dependences, which are those observed when a dependence is established as a result of the need for an alternative way for receiving a needed service. One example of conditional dependence is when communication facilities need the provision of transportation services to have their backup power generators refueled in order to keep their equipment powered during long power outages. These and other aspects related to dependencies, including the description of the important concept of service buffering, are discussed in detail in Chapter 4.

Various terms are often associated to the concept of resilience. As was already discussed, resilience is sometimes associated to the concepts of reliability, availability, and maintainability. However, as was explained, reliability and resilience are different concepts. One of the main differences is that resilience applies to a particular uncommon event, whereas reliability requires normal operating conditions. Such a difference makes it possible to envision a power grid that is "reliable" (from the conventional understanding of the term "reliability" applicable to electric power distribution grids) because it experiences very few outages during normal operation, but is not resilient

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

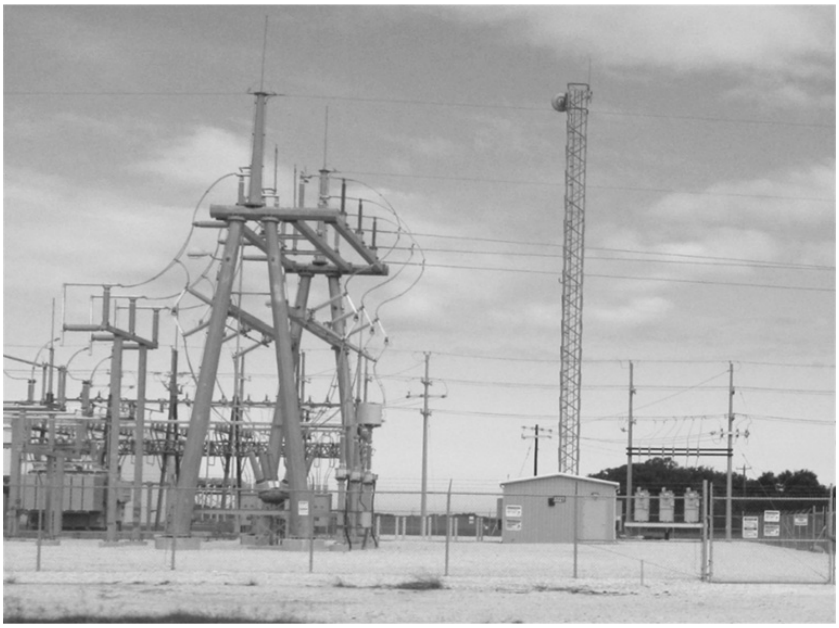

Figure 1.6 A communications microwave antenna belonging to the electric grid for transmitting sensing and control data on top of a tower behind an electric power substation control house on the right.

because, when an extreme event happens, the resulting outage affecting almost all of the customers is excessively long. Likewise, it is possible to think about a power grid that is resilient because it is possible to recover service very quickly after a disruptive event, but that is not reliable because of the many serious outages experienced during normal operation. Still, it is possible to find resilience definitions that could be considered incorrect within the context discussed in this book because they are based on reliability, availability, and maintenance terms. This incorrect use of the term resilience has been particularly observed in the field of computing systems in which resilience has been associated with fault tolerance and dependability [31]. In a related work "dependability" is defined as the "delivery of service that can justifiably be trusted, thus avoidance of failures that are unacceptably frequent or severe" [32]. In [31] this definition of dependability is used to provide an alternative definition of resilience as "the persistence of the avoidance of failures that are unacceptably frequent or severe, when facing changes" or, in short, that resilience is "the persistence of dependability when facing changes." The fact that these definitions of resilience refer to frequent failures and that the concept of recovery speed is not considered makes these concepts of resilience unrelated to the proper understanding of the term resilience that has been discussed earlier in this chapter. Another related definition of resilience, also presented in [31], is that resilience is "the persistence of service delivery that can be justifiably be trusted, when facing changes." Although this definition of resilience is not applicable within the context used in this book because

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

it still considers normal operating conditions or a standard set of operating conditions, the notion of relating resilience to the delivery of a service helps us to connect the definition of resilience from [23] used in this book with the aforementioned critical infrastructure model based on service delivery and with some resilience quantitative metrics that are discussed in detail in Chapter 3. That is, the definition of resilience from [23] indicates what resilience is based on the characteristics of a resilient system, but such a definition does not provide an indication of how resilience is assessed in a quantitative way. Since the proposed model for a critical infrastructure system is based on service provision, then one way of measuring resilience is by evaluating service delivery performance through one or more of the service delivery attributes, such as, for example, quality of service.

Another term that has been associated with resilience is that of robustness. However, there is no consistency in the definition of robustness. While in [32] robustness is considered a dependability attribute defined as "persistence of dependability with respect to external faults" and, thus, still relates such a concept more to reliability characteristics than to the resilience property, the same author in [31] recognizes that robustness and resilience are applicable to uncommon events when citing [33], which indicates that "a computing system can be said to be robust if it retains its ability to deliver service in conditions which are beyond its normal domain of operation." This more appropriate definition of robustness within the context of this book can be considered similar to that found in [34], which denotes robustness as "the degree to which a system is able to withstand an unexpected internal or external event or change without degradation in system's performance." These two definitions for robustness are similar to that of resistance given in [35] as "the capacity of withstanding the disruptive effects of a given event." That is, robustness or resistance is associated to the withstanding characteristic of a critical infrastructure to the disruptive actions of an uncommon event.

Fragility is another concept associated to resilience and, as detailed in Chapter 3, used in several approaches to identify a metric for resilience. In these cases, fragility is typically used through fragility curves or fragility functions that describe "the probability of failure of a structure or structural component, conditional on a loading that relates the potential intensity of a hazard" [36]. That is, from [35] fragility is understood as "the failure probability . . .. with respect to the intensity of the hazard."

Vulnerability is another important concept that it is related to system resilience. In many definitions, vulnerability is related to adaptability or adaptive capacity. In [26] adaptability is defined as "the ability to incorporate lessons learned from past events to improve resilience." Similarly, [37] defines adaptive capacity as "the ability of institutions and networks to learn, and store knowledge and experience." In [37] vulnerability is defined as "pre-event, inherent characteristics of the social system that create the potential for harm." Although this definition characterizes vulnerability as a pre-event characteristic, the notion of harm is unclear. Several definitions of vulnerability are presented in [38]. Like in [37] and in [39], many of these definitions relate vulnerability to the concepts of sensitivity and exposure in addition to that of adaptive capacity.

https://doi.org/10.1017/9781108648899.002 Published online by Cambridge University Press

In [39] exposure is the "degree, duration and/or extent in which the system is in contact with, or subject to, the perturbation," whereas sensitivity is "the degree to which the system is modified or affected by an internal or external disturbance or set of disturbances." Also [39] indicated that sensitivity "can be measured as the amount of transformation of the system per unit of change in the disturbance," or, mathematically, as the result of dividing a transformation by a perturbation without providing a means for measuring those two functions. Another definition of vulnerability, which is arguably simpler and more suitable for the context in which it is applied in this book, was presented in [40], which defines vulnerability as "the degree to which a system, or part of it, may react adversely during the occurrence of a hazardous event." Hence, in this book vulnerability is similarly considered as how much more or less susceptible a given community system or part of it is to provide the same service provision resilience than a reference standard community system or part of it when both are subject to a hazard with the same intensity. This definition is a modified version of the one provided in [35].

Many other terms can be found in the literature to be associated to that of resilience. For example, [26] defines resourcefulness as "the ability to skillfully manage a crisis as it unfolds." Many other terms, such as *extensible*, *composable*, *evolvability*, *assessability*, *usability*, and *extensibility*, are also presented in [41], although their use tends to add confusion because of a lack of an existing definition – in some cases some of these terms are not even found in dictionaries – without significantly contributing to the focus of the discussion. However, since the origin of the term resilience is found in the materials science field, it is interesting to mention the use of the term brittleness in [35] within the context of resilience. In the materials science field, a material is brittle when, subjected to stress, it breaks without significant plastic deformation. The opposite of brittleness is ductility. A ductile material has the ability to deform before breaking [42]. In practical terms, a ductile material has a higher modulus of toughness (see Fig. 1.1) than a brittle material and, thus, for the same stress a brittle material tends to break with much less deformation than a ductile material. That is, a brittle material tends to fracture much faster than a ductile material when subject to the same stress. In the context of community systems resilience, resistance provides somewhat of an analogy to these terms, but resistance does not completely convey an idea of deformation, which is part of the concepts of brittleness and ductility. Such relationships are considered in [35], in which "brittleness relates the level of disruption with respect to the damage suffered by the power grid in a given area." This definition can be extended to any community system, providing an idea of how much a system-provided service maintains performance (or "deforms without breaking") when experiencing a given damage level (or "stress"). Those systems able to have less disruption for the same damage level are systems that can be considered more ductile because, within the specific context of the use of brittleness in here, a service disruption could be interpreted as the failure point of a service provision. In the case of a power grid, such as that indicated in [35], a lower percentage of customers experiencing an outage for the same level of damage indicates a system that is more ductile.

References

[1] Merriam-Webster Dictionary, "Resilience." www.merriam-webster.com/dictionary/resilience.

[2] J. M. Gere and B. J. Goodno, *Mechanics of Materials*, 8th edition, Cengage Learning, Stamford, CT, 2013.

[3] J. M. Gere, *Mechanics of Materials*, 6th edition, Brooks/Cole–Thomson Learning, Belmont, CA, 2004.

[4] J. C. Trautwine, *The Civil Engineer's Pocket-Book: of Mensuration, Trigonometry, Surveying, Hydraulics, etc*., 13th edition, J. Wiley & Sons, New York, 1888.

[5] J. Par, T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkov, "Integrating risk and resilience approaches to catastrophe management in engineering systems." *Risk Analysis*, vol. 33, no. 3, pp. 356–367, Mar. 2013.

[6] P. Guthrie and T. Konaris, *Infrastructure Resilience*, UK Government Office of Science, London, Nov. 2012.

[7] C. Gallego-Lopez and J. Essex (with input from Department for International Development), "Designing for Infrastructure Resilience: Evidence on Demand," UK Department of International Development report, July 2016.

[8] D. L. Alderson, G. G. Brown, and W. M. Carlyle, "Operational models of infrastructure resilience." *Risk Analysis*, vol. 35, no. 4, pp. 562–585, Apr. 2015.

[9] A. Kwasinski and V. Krishnamurthy, "Generalized Integrated Framework for Modeling Communications and Electric Power Infrastructure Resilience," in Proceedings of INTELEC 2017, Oct. 2017.

[10] A. Kwasinski, "Field Damage Assessments as a Design Tool for Information and Communications Technology Systems That Are Resilient to Natural Disasters," in Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), Barcelona, Spain, 6 pages, Oct. 2011.

[11] A. Kwasinski, "Field Technical Surveys: an Essential Tool for Improving Critical Infrastructure and Lifeline Systems Resiliency to Disasters," in Proceedings of the IEEE 2014 Global Humanitarian Technology Conference, San Jose, CA, pp. 78–85, Oct. 2014.

[12] M. N. Albasrawi, N. Jarus, K. A. Joshi, and S. S. Sarvestani, "Analysis of Reliability and Resilience for Smart Grids," in Proceedings of the 2014 IEEE 38th Annual Computer Software and Applications Conference (COMPSAC), July 2014.

[13] J. A. Momoh, S. Meliopoulos, and R. Saint, "Centralized and Distributed Generated Power Systems – A Comparison Approach," PSERC Publication 12–08, June 2012.

[14] Y. Haimes, K. Crowther, and B. Horowitz, "Homeland security preparedness: balancing protection with resilience in emergent systems." *Systems Engineering*, vol. 4, no. 11, pp. 287–308, Sept. 2008.

[15] V. Krishnamurthy and A. Kwasinski, "Characterization of Power System Outages Caused by Hurricanes through Localized Intensity Indices," in Proceedings of the 2013 IEEE Power and Energy Society General Meeting, July 2013.

[16] Severe Impact Resilience Task Force, "Severe Impact Resilience: Considerations and Recommendations," North American Electric Reliability Corporation (NERC) report, May 2012.

[17] J. D. Taft, "Electric Grid Resilience and Reliability for Grid Architecture," Pacific Northwest National Laboratory report PNNL-26623, Nov. 2017.

[18] A. Kwasinski, W. Weaver, and R. Balog, *Micro-grids in Local Area Power and Energy Systems*, Cambridge University Press, Cambridge, 2016.
[19] IEEE Standards Association (IEEE SA), "IEEE Guide for Electric Power Distribution Reliability Indices," IEEE Std 1366–2003 (Revision of IEEE Std 1366–2003), 2004.
[20] North American Electric Reliability Corporation (NERC), "Understanding the Grid," Aug. 2013.
[21] North American Electric Reliability Corporation (NERC), "Definition of Adequate Level of Reliability," Dec. 2007. www.nerc.com/docs/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf, last accessed January 30, 2019.
[22] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, *Power Generation, Operation, and Control*, 3rd edition, John Wiley & Sons, Hoboken, NJ, 2014.
[23] US White House, President Barack Obama Presidential Policy Directive/PPD21 "Critical Infrastructure Security and Resilience," Feb. 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, last accessed May 25, 2015.
[24] Governments of Australia, Canada, New Zealand, the United Kingdom, and the United States of America, "Critical Five; Forging a Common Understanding for Critical Infrastructure: Shared Narrative." Mar. 2014.
[25] National Research Council *Disaster Resilience: A National Imperative*. The National Academies Press, Washington, DC, 2012.
[26] A. R. Berkeley III and M. Wallace, "A Framework for Establishing Critical Infrastructure Resilience Goals," report of the National Infrastructure Advisory Council (NIAC), Washington, DC, Oct. 2010.
[27] D. Rehak, P. Senovsky, and S. Slivkova, "Resilience of critical infrastructure elements and its main factors." *Systems*, vol. 6, no. 2, June 2018.
[28] L. Marlowe, "Strong opposition to overhead lines in France." *The Irish Times*, June 24, 2014. www.irishtimes.com/news/ireland/irish-news/strong-opposition-to-overhead-lines-in-france-1.1842855, last accessed January 30, 2019.
[29] A. Kwasinski, J. Trainor, B. Wolshon, and F. M. Lavelle, *A Conceptual Framework for Assessing Resilience at the Community Scale*, NIST GCR 16–001, Jan. 2016.
[30] US Department of Homeland Security, "NIPP 2013. Partnering for Critical Infrastructure Security and Resilience." 2013.
[31] J.-C. Laprie, "From Dependability to Resilience," in the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2008, Anchorage, AK, June 2008.
[32] J.-C. Laprie, "Dependability and Resilience of Computing Systems." Presented at the 2nd International Workshop on Software Engineering for Resilient Systems (SERENE'10), London, Apr. 2010.
[33] T. Anderson (Ed.), *Resilient Computing Systems*, Collins, London, 1985.
[34] I. Linkov, D. A. Eisenberg, K. Plourde et al., "Resilience Metrics for Cyber Systems." *Environment Systems and Decisions*, vol. 33, no. 4, pp. 471–476, Dec. 2013.
[35] A. Kwasinski, "Numerical Evaluation of Communication Networks Resilience with a Focus on Power Supply Performance during Natural Disasters," in Proceedings of INTELEC 2015, Osaka, Japan, Oct. 2015.
[36] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and

adaptation measures." *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3747–3757, Sept. 2017.

[37] L. Colburn and T. Seara, "Resilience, vulnerability, adaptive capacity, and social capital," presented at 2nd National Social Indicators Workshop, Silver Spring, MD, Sept. 2011.

[38] Y. Lei, J. Wang, Y. Yue, H. Zhou, and W. Yin, "Rethinking the relationships of vulnerability, resilience, and adaptation from a disaster risk perspective." *Natural Hazards*, vol. 70, no. 1, pp. 609–627, Jan. 2014.

[39] G. C. Gallopin, "Linkages between vulnerability, resilience, and adaptive capacity." *Global Environmental Change*, vol. 16, no. 3, pp. 293–303, Aug. 2006.

[40] V. Proag, "The concept of vulnerability and resilience." *Procedia Economics and Finance*, vol. 18, pp. 369–376, 2014.

[41] J.-C. Laprie, "Resilience for the Scalability of Dependability," in Proceedings of the Fourth IEEE International Symposium on Network Computing and Applications (NCA'05), Cambridge, MA, July 2005.

[42] University of Virginia, "MSE-209 Spring 2004. Chapter 6 Mechanical Properties of Materials." www.virginia.edu/bohr/mse209/chapter6.htm, last accessed January 30, 2019.