Chapter 3
Assessing Dependability and Resilience in Critical Infrastructures: Challenges and Opportunities

Alberto Avritzer, Felicita Di Giandomenico, Anne Remke and Martin Riedl

Abstract Critical infrastructures (CI) are very complex and highly interdependent systems, networks and assets that provide essential services in our daily life. Most CI are either built upon or monitored and controlled by vulnerable information and communication technology (ICT) systems. Critical infrastructures are highly interconnected systems and often use common ICT components and networks. Therefore, cascading faults and failures are likely events in critical infrastructures. Moreover, such failures can easily spread to other infrastructures and can possibly span to other countries or even continents. Assessing resilience is thus a cornerstone for improving the dependability in critical infrastructures. Due to the complexity and interdependency of such systems many different challenges and opportunities surface when developing methods and tools for resilience assessment. During the last decade both academia and industry developed an increased interest in this research area and a variety of projects with different focus started to emerge. This chapter gives an overview about the main requirements for resilience assessment and discusses the state of the art and emerging research directions. To exemplify the diversity of this

A. Avritzer (✉)
Siemens Corporate Research and Technology,
755 College Road East, Princeton, NJ 08540, USA
e-mail: alberto.avritzer@siemens.com

F. Di Giandomenico
ISTI Department, Italian National Research Council,
via Moruzzi 1, 56124 Pisa, Italy
e-mail: digiandomenico@isti.cnr.it

A. Remke
University of Twente,
Enschede, The Netherlands
e-mail: anne@cs.utwente.nl

M. Riedl
Universität der Bundeswehr München,
Neubiberg, Germany
e-mail: martin.riedl@unibw.de

K. Wolter et al. (eds.), *Resilience Assessment and Evaluation of Computing Systems*,
DOI: 10.1007/978-3-642-29032-9_3, © Springer-Verlag Berlin Heidelberg 2012

research area a special focus is put on different sub-fields with increasing granularity from the fairly general interdependency modeling to the reliability modeling of a Smart-Grid distributed automation network.

3.1 Introduction

More and more, our society and economy rely on the well-operation of a number of infrastructures, which regulate critical processes and provide vital services. Critical infrastructures (CI) span a number of critical sectors, including: public health and safety, energy, water, information and telecommunications, emergency services, agriculture and food, transportation, banking and finance, government, and many others. Over the last 10–15 years, the role of information and communication technology (ICT) in society has dramatically changed. Where some 15 years ago, ICT supported some business and stand-alone office processes, ICT now forms the heart of these processes. Moreover, ICT now plays an important role in most processes and services in our economy, however, often hidden behind a non-ICT-like user interface. A key example of the latter is the role of ICT in critical infrastructures. The non-functioning of critical infrastructures has a vast impact on economic and social welfare. Hence, for such infrastructures it is essential to be resilient against faults and failures and to survive catastrophic events.

This chapter focuses on ICT-based critical infrastructures from the point of view of their dependability and resilience assessment. As reported in the "critical infrastructure resilience final report and recommendations" produced by the US NIAC [677], resilience has become an important dimension of the critical infrastructure protection mission, and a key element of the value proposition for partnership with the government because it recognizes both the need for security and the reliability of business operations. Although each critical infrastructure sector operates differently, a common definition of infrastructure resilience is needed for public policies and governance to be effective. Toward this end, the NIAC has developed the following definition based on discussions with executives and security experts across many sectors: *infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate*, *absorb*, *adapt to*, *and/or rapidly recover from a potentially disruptive event*.

Research has shown that many critical infrastructures are interrelated. Especially ICT infrastructures play an important role in the vitality of other infrastructures, e.g., the transport infrastructure does not operate properly without a reliable ICT infrastructure. These dependencies can cause cascades of failures that start with simple defects in one type of system, and may finally lead to disasters in other infrastructures. Therefore, there is a growing need to analyze the chains of influence that cross multiple sectors and that can induce potentially unforeseen secondary effects. This reinforces the importance to consider dependability and resilience as

a component of critical infrastructure protection strategy and to devise appropriate methodologies and techniques to promote its analysis and assessment.

This chapter on critical infrastructures points out the requirements for resilience assessment of this challenging and crucial sector, pointing out relevant studies already performed and indicating promising directions for future work. A more concrete approach to resilience analysis in the CI field is provided in the Chap. 18 in this book.

The outline of the remainder of the chapter is as follows. Section 3.2 discusses the requirements for resilience assessment of critical infrastructures. Section 3.3 presents an overview of the literature on critical infrastructures assessment approaches. A significant effort is nowadays devoted to interdependencies modeling and analysis. Section 3.4 reviews some relevant studies in this field. Section 3.5 focuses on how stochastic hybrid models can be used for the dependability evaluation of fluid critical infrastructures. This section provides an interesting example of the similar feature characteristics between critical infrastructures in different domains. Increasing the level of detail, Sect. 3.6 presents a concrete case study to illustrate a reliability assessment approach for a distributed automation smart-grid distribution network. Emerging directions for research in critical infrastructures are presented in Sect. 3.7.

3.2 Requirements for Resilience Assessment of Critical Infrastructures

Critical infrastructures are often controlled by a supervisory control and data analysis (SCADA) [857] system, which is potentially vulnerable to attacks and misuse. SCADA systems consist of sensors, actuators, controllers and a human-machine interface (HMI) through which human operators control the physical process. It is important to correctly capture interdependencies that arise between the SCADA network and the physical network, but also interdependencies between different critical infrastructures. Interdependency assessment is discussed in Sect. 3.2.1. Modeling formalisms have to be able to capture the complex nature of critical infrastructures; requirements with respect to, e.g., scalability, heterogeneity and compositionality are presented in Sect. 3.2.2. Measures that can be used to evaluate the resilience of such systems have to be defined in a sound and unambiguous way. Different types of evaluation are highlighted in Sect. 3.2.3. Possible faults range from the malfunctioning of SCADA components to cyber attacks and are summarized in Sect. 3.2.4.

3.2.1 Interdependencies

There is a consensus in the literature on critical infrastructures that interdependency analysis is of paramount importance to improve the resilience, survivability and

security of these vital systems. An interdependency is a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other [778]. Infrastructure interdependencies can be categorized according to various dimensions in order to facilitate their identification, understanding and analysis. Among the most important dimensions identified in [778] are: (a) the couplings among the infrastructures and their effects on their response behaviour (loose or tight, inflexible or adaptive), (b) the state of operation (normal, stressed, emergency, repair), and (c) the type of failure affecting the infrastructures (common-cause, cascading, escalating).

Interdependencies increase the vulnerability of the corresponding infrastructures as they give rise to multiple error propagation channels from one infrastructure to another that increase their exposure to accidental as well as to malicious threats. Consequently, the impact of component failures in critical infrastructures can be exacerbated due to interdependencies and the overall severity of a failure is generally much larger and more difficult to foresee, compared to failures confined to single infrastructures. As reported in [742], past major power grid blackouts have been initiated by a single event (or multiple related events such as an equipment failure of the power grid that is not properly handled by the SCADA system) that gradually led to cascading outages and eventually to the collapse of the entire system.

Analyzing interdependencies allows a greater understanding of the effects of failures. Three types of failures are of particular interest when analyzing interdependent infrastructures: (1) cascading failures, (2) escalating failures, and (3) common cause failures. Cascading failures occur when a failure in one infrastructure causes the failure of one or more component(s) in a second infrastructure. Escalating failures occur when an existing failure in one infrastructure exacerbates an independent failure in another infrastructure, increasing its severity or the time for recovery and restoration from this failure. Finally, common cause failures occur when two or more infrastructures are affected simultaneously because of some common cause.

3.2.2 Modeling Formalism

The large and complex nature of critical infrastructures with a multiplicity of interactions and types of interdependencies involved requires a very flexible compositional modeling framework that is able to accommodate different levels of abstraction. To analyze their safety and survivability in the presence of disasters advanced structuring, monitoring and assessment methods are necessary. From the modelling point of view, abstraction layers and modular, hierarchical and compositional approaches are viable directions to cope with these aspects. New model classes and languages are necessary to accurately describe the structure and behavioral dependencies in critical infrastructures. Which modeling methods are suitable for which infrastructure? Which are the crucial system issues to accurately model per infrastructure? Expert knowledge will be necessary to establish critical subsystems and sensible parameters settings; sensitivity analyses can be used to distinguish the crucial parameters, thereby

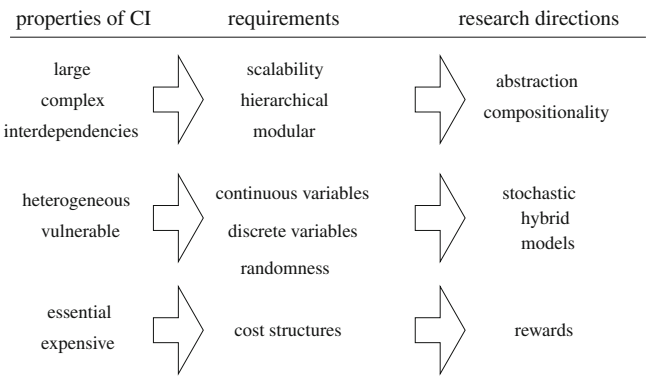


Fig. 3.1 Properties of critical infrastructures, requirements for modeling and emerging research directions

keeping the state space of the models as small as possible. As critical ICT infrastructures are very big systems, scalability is an important issue in modeling and analysis.

Figure 3.1 illustrates how the most prominent properties of critical infrastructures lead to certain modeling requirements and hence, to research directions that are expected to improve the state of the art in the field. Details are given in the following.

When modeling these complex systems [300] not all parameters and not all usage patterns are known exactly. Moreover specific details of vulnerabilities and failures will be unknown at design time, such as the mean time to failure and the impact of a given vulnerability. In such cases it is appropriate to make stochastic assumptions about the system and the disaster behavior. Hence, modeling formalisms that have been shown useful to model large-scale computer and communication systems, e.g., stochastic process algebra and stochastic Petri net, can be used to formally describe critical infrastructures, their inter-dependencies, and their cost structure.

The heterogeneity of typical critical infrastructures may require a combination of different formalisms/techniques to describe the various components of a system and their dependencies. For example, the combination of continuous and discrete phenomena may need to be captured in the modeling framework. Examples of discrete quantities are the number of spare parts and the state of sensors, actuators and ICT-components, whereas the continuous variables represent quantities, like the amount of produced energy, or the quality of treated water in terms of temperature and pressure. Hence, a modeling formalism is needed that allows describing both discrete and continuous quantities. Due to the flexible combination of discrete and continuous state components, Stochastic Hybrid Models (SHMs) can be a natural choice to accurately model both the process automation and the production process which is the essential part of several critical infrastructures.

The cooperation among subsystems of different nature inside the same Critical Infrastructure or among cooperating critical infrastructures requires advanced methods to reconcile different aspects under a common development and assessment framework. In this context, the studied infrastructures are assembled from many

heterogeneous subsystems with different specifications, operation phases, and regimes. Therefore, a common framework has to be able to combine the different structural and quantitative aspects of critical infrastructures. Compositional modeling [141, 859] can simplify the modeling process and can lead to intuitive formalisms. Compositional analysis reduces the complexity of verification. Changes in the system then only affect the modified component and not the complete model. Compositional analysis is a challenging topic that requires additional research.

3.2.3 Type of Evaluation

The Evaluation of critical infrastructures has to address functional properties like inter-dependencies, deadlocks, etc., as well as extra-functional (quantitative) properties. As an example of the latter, what is the probability that 10 min after the occurrence of a given disaster, a basic service level is again available for 80 % of the user population? Not all infrastructures are critical and not all critical infrastructures have the same level of criticality. An evaluation process is required to identify vulnerabilities, interdependencies and interoperabilities between systems, to understand what specific assets of the addressed CI are utmost critical and need to be protected the most. Following this evaluation, steps can be taken to mitigate the identified vulnerabilities. For example, if an electric substation is damaged leading to a blackout, complications are experienced by a number of other systems/infrastructures and by the services they provide, like railroad operations causing a decreased movement of commodities and potential complications for emergency services. Thus, that electric substation must be protected not only for the Energy Sector, but also for the safeguarding of other sectors' infrastructure. Clearly, properties to be considered as indicators of the resilience of the Critical Infrastructure under study may vary significantly depending on the specificity of the targeted sector. The evaluation method should therefore be able to specify and assess resilience indicators according to the sector's needs, addressing both the interest of system designers and operators as well as users requesting services to the infrastructure.

Safety is defined as the absence of catastrophic consequences on the user(s) in their environment [63]. Safety analysis of vital infrastructures encompasses the classification of different types of disasters, according to their probability of occurrence and their effect on the controlled process; one can think of the degree of damage regarding time, space and monetary costs, in addition to the probability of cascading failures. Generally speaking, disasters can also be the result of malicious attacks or even terrorism. Thus, security of critical infrastructures is an important issue to deal with. Hence, combining the necessary expertise on network security (especially intrusion detection) and on system modeling and analysis is necessary to forecast the consequences of security attacks. This will help in finding the right counter measures and to develop recovery strategies.

Dependability has been defined as the ability to deliver service that can justifiably be trusted [63]. Given detailed models of the critical infrastructures, the dependabil-

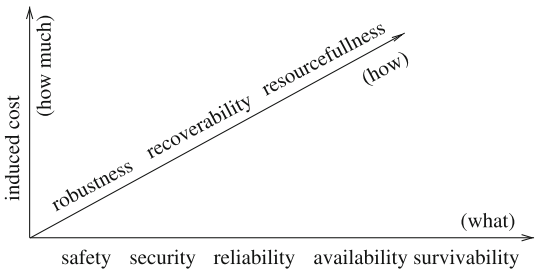


Fig. 3.2 Building a more resilient infrastructure comes at a certain cost

ity of the system can be evaluated with analytical techniques or using simulations. It is of utmost importance to use clear and formally defined notions of dependability. For example, survivability [300] is defined as a system's ability to recover predefined levels of service in a timely manner. Survivability evaluation then encompasses the evaluation of the probability (distribution) that predefined service levels are reached within a certain time, given the recent occurrence of a disaster of some form. Survivability evaluation deliberately only addresses the system recovery process; the process toward the disaster is explicitly not modeled, but taken as given. After the classification of disasters through safety analysis, a so-called Given Occurrence Of Disaster (GOOD) model of the system under study can be built and used for survivability analysis. Clearly, the recovery following a disaster highly depends on the type and extent of the disaster as well as on the affected infrastructure and built-in recovery mechanisms.

Other approaches from the field of dependable system design to achieve high-dependability (reliability and availability) can be useful in the context of critical infrastructures, such as implementing smart recovery strategies or introducing redundancy of some form [543]. As introduced in [677], it can be useful to divide resilience into *robustness*, *recoverability* and *resourcefulness*. Clearly, building a more resilient system comes at a higher price, so what is the relation between increased costs and increased resilience? Where does the point of diminishing returns lie? What is technically possible at which costs?

Figure 3.2 illustrates the relationship between a system's extra-functional requirements/properties, i.e., (**what**), the architecture features that are constructed to make the system more resilient, i.e., (**how**), and the associated costs to build a resilient system, i.e., (**how much**). As an example of this tradeoff, one might consider intrusion tolerance techniques and compare them to the objective of completely avoiding intrusions. Intrusion tolerance techniques are more likely to be successful in practice and may be less costly and more practical to implement, e.g. through redundancy. The implementation of a more practical approach increases the system's robustness and can be measured, e.g., in safety and security. Minimizing the time to recovery through smart repair schedules increases the recoverability of the system and will lead to higher availability and survivability. Comparing infrastructure designs alternatives with respect to their survivability and dependability will lead to more informed design decisions and hence, to more resourceful infrastructures.

3.2.4 Type of Faults

For each vital infrastructure a variety of possible disasters has to be considered. In case of a network infrastructure, a disaster can be a power outage, or it can be an explosion demolishing parts of the system. Both accidental and malicious faults need to be accounted for in the analysis. In previous decades, accidental threats were basically the only real threats facing infrastructure, especially natural disasters, which tend to be localized to one region and have a fixed and, at times, predictable duration. Until the bombing of the Murrah Federal Building in Oklahoma City in 1994, low attention was devoted to malicious acts targeting these critical components. In more recent years, preparation for Y2K (2000), fall-out from post-9/11 events, and a series of blackouts of the power systems experienced both in the US and in Europe have all reinforced the evidence of how vulnerable these systems are or can become to human attacks. Cyber attacks to the ICT systems that are controlling critical infrastructures are becoming more and more prominent. As an example, consider what happened in Australia [754] in 2001: a hacker broke into the network of a water treatment plant, opened an emergency valve and started to pump one million liters of raw sewage into the city parks. We could provide many other similar examples, such as the recent Stuxnet-worm [331, 520] which poses a serious thread to computers controlling industrial processes in the energy sector, or the Aurora attack on power generators [645] where the system could hurt itself via unauthorized SCADA commands.

A so-called threat or failure model [495] can be built, encompassing information on the type of failures that can be expected, their frequency, their duration and their intensity (e.g., computational strength). Because failures may be dependent on the system state, such a dependence has to be formulated as part of the model as well. Similarly, countermeasure models can be created, taking into account the incurred costs (monetary, or otherwise) of taking the countermeasure and its effect on the productivity of the infrastructure.

Heterogeneity also needs to be addressed at the level of vulnerability exposed by the different subsystems composing a critical infrastructure, e.g. the use of subsystems, such as Wireless SCADA, which are known to be typically vulnerable to error and misuse. In fact, advances in technology and SCADA systems have enhanced critical sector operations but created additional vulnerabilities, which must be addressed to adequately protect the critical infrastructure.

3.3 State of the Art in Resilience Assessment of CI: General Overview

The last decade saw significant research opportunities in resilience assessment of critical infrastructures. One of the important characteristics of critical infrastructure that contributes to its complexity is heterogeneity. Therefore, related work focuses on different aspects, such as the spatial distribution, interdependencies, uncertainty,

non-linearity or hybrid systems. The evaluation is mainly focused on vulnerability, risk, and recoverability. It is performed using qualitative and quantitative assessment methodologies.

In the following we overview existing methods and techniques for CI assessment, providing a rough classification into qualitative and quantitative approaches. Due to the sheer amount of related work, completeness cannot be achieved - for more overview papers, please refer to [339, 376, 962].

Qualitative assessment approaches are discussed in Sect. 3.3.1 and quantitative approaches in Sect. 3.3.2. Section 3.3.3 gives an overview of ongoing projects in critical infrastructures.

3.3.1 Qualitative Assessment Approaches

Qualitative assessment approaches are descriptive in nature and aim at an in-depth understanding of the critical infrastructure under study. In the following, we discuss several approaches for qualitative vulnerability and risk assessment.

Qualitative vulnerability assessment can help to better understand the nature of vulnerabilities and to identify common causes of major failures. In the following we present two approaches to illustrate the application of qualitative vulnerability assessment to water cleaning systems and to electric power systems.

The Infrastructure Vulnerability Assessment Model (I-VAM) [328] proposes a qualitative treatment of the vulnerability of water cleaning systems. System experts have to establish value functions and weights and they have to assess protection measures of the system. Simulation (Monte-Carlo and Latin Hypercube) is used to analyze the sensitivity of the model and to obtain a vulnerability density function.

In [45] it is claimed that blackouts in electrical power systems are seldom caused by the failure of a single equipment but instead caused by cascading effects that cannot be predicted. There, structural vulnerability is classified into *node-* (e.g., substation) and *plain vulnerability* (e.g., transmission line). Moreover, different types of vulnerability indices are proposed for different kind of operating parameters based on over-limit information, regulating information, loss of load, and sensitivity analysis. The authors provide methods to calculate different kinds of indices to assess an electrical power system concerning its vulnerability after an out of service condition for a substation or a group of tie lines.

Qualitative risk assessment aims to identify the qualitative value of risk regarding a certain situation and threat under certain assumptions and uncertainties. Qualitative risk assessment approaches are often used to identify targeted threats, e.g., cyber-attacks. In the following we present a review of related work on inductive and deductive risk assessment, fault and attack trees, tableau-based and ontology-based approaches.

Inductive risk assessment methods, such as event tree analysis (ETA), start from certain observations (e.g., a particular hazard) within the system and try to inductively find its consequences. In [16] event tree analysis has been applied as a systematic

approach to investigate scenarios within a 3-step methodology. There, the consequences of the event of hurricane Hazel have been modeled. Each branch of the tree leads from a prior event to more specific outcome. The elements rainfall, flood and wind have been depicted in the first level, resulting in consequences concerning certain rivers or infrastructural damage. Based on the insights a flooding model for the Humber river has been developed based on GIS information (i.e., digital elevation maps). Moreover a knowledge base with interdependency relations has been developed.

Deductive risk assessment methods on tree-based structures (e.g., fault-tree, attack-tree effect, tree analysis, cause-consequence analysis) work in the opposite way, i.e., from general to more specific. In [874] a new algorithm based on attack-trees as simplified methodologies for impact analysis has been developed for the evaluation of cyber-security incorporating password policies and port auditing. The root node represents the ultimate goal (e.g., getting access) of an attack. Different subgoals can be formulated as intermediate nodes that are combined over "AND" and "OR" nodes. A leaf node can be an element of an intrusion scenario including defense nodes as successors. First, cyber-security conditions are measured corresponding to a number of assumed values reflecting the severity of vulnerability. Then, the attack tree is formulated concerning the identified attack objectives, cyber-security conditions and countermeasures. Finally, the system vulnerability is derived from the computed leaf vulnerabilities of the attack tree and the specific scenario associated with the attack.

To incorporate both random failures and deliberate acts, [672] combines *fault-trees and attack trees*. Fault-trees are traditionally used to calculate the reliability of systems, whereas attack trees enrich the fault tree by malicious attack patterns. Attacks can cause several types of events that are classified as basic, intermediate, or top events, depending on the event position in the attack tree. Top events result in an overall critical infrastructure failure. The authors argue that an attack tree goal is equivalent to a fault tree event, where the difference lies in its origin (i.e., originated by a malicious agent or random events). To use extended fault-trees, the measures resulting from the attack trees must be quantified in terms of event probabilities. This is done by deriving the probability of basic events from assumptions concerning the motivation and resources of threat agents, environmental conditions and subjective probabilities associated to the elements of the attack tree.

Often, simple *tableau-based* approaches are used for qualitative risk assessment. For example, in [13] the FEMA defines a tableau based approach to mitigate terrorist attacks against buildings. Global vulnerability is quantified according to a reference scale. Asset values are assessed based on a parameters scaling between very low and very high. Event profiles for terrorism and technological hazards are defined and a matrix representation of the asset vulnerability is presented. The tools provided can help decision makers decide which types of threats they want to counter after risk assessment is made for each threat.

There is also work available that uses *ontology-based* decision support tools for critical infrastructures, i.e., with underlying description logics. Ontologies provide a way to represent domain knowledge in the form of classifications and relationships.

Automated deduction algorithms allow for reasoning about potential vulnerabilities and threats. In [211] such an ontology-based approach is taken as part of the INSPIRE project, which aims to increase security and protection through infrastructure resilience. Vulnerabilities due to the integration of IT and SCADA systems are explored together with connections, dependencies, and security aspects of SCADA systems (e.g., inherent vulnerabilities and effects). An OWL-DL ontology representing physical and logical assets, safeguards, threats, sources of attack, and vulnerabilities is described. These elements are connected through different types of relations (e.g., `Vulnerability` "is exploited by" `Threats`, `Asset` "has vulnerability" `Vulnerability`). Instances of certain CI infrastructures can be developed and queried using a query language by applying the underlying deduction algorithms. One example of a query language is SWRL. Questions such as "If I have resources A,B and C what kinds of attacks should I expect?" can be posed and answered by the implemented query mechanism.

3.3.2 Quantitative Assessment Approaches

Quantitative assessment uses measurable data to analyze and improve resilience or aims at computing quantitative performance measures, such as survivability, reliability, or efficiency. In the following, we review some quantitative assessment approaches using statistical analysis, stochastic models, and testbeds.

Statistical analysis. Critical infrastructure disruption events that cascaded across CI boundaries are examined in [612]. A *disruption event database* has been built as an empirical database, using publicly available data, which can be used for the understanding of cascading effects. It has been established that such effects mainly originate from energy and telecommunication. The dependencies are very focused and directional. The authors therefore question the domino theory since they only found very rare events which result in deep level cascades.

An extension to *data farming* is used in [280] to generate different types of network topologies. Simulation experiments with random and targeted terrorist attacks are performed. The results show that most networks start to fail when the number of attacks is larger than an empirically defined measure of node connectivity. Random network topologies seem not to be as robust as scale-free networks.

Stochastic models. An important formalism used in stochastic modeling is Stochastic Activity Networks [805]. This formalism has been applied in [115] as an approach for quantitative interdependency analysis in the context of large and complex CIs. The papers focus is on how the occurrence and size of cascades changes, when the strength of interdependencies is varied. The Möbius tool [225] is used to simulate the Stochastic Activity Network models using event-driven Monte-Carlo Simulation. The modeling process consists of determining the distribution of the cascade size, followed by an assessment of the impact of model abstraction and refinement on the quality of the results obtained in the analysis.

In [873] the risk of cyber attacks on the power system is calculated as the product of two factors: the probability of a successful intrusion and the impact of the intrusion as loss of power due to an unexpected loss of electric load. The two risk factors are evaluated by two separate techniques. The cyber layer underlying the substation control systems is analysed through stochastic firewall and password models, while the impact factor for the attack upon a SCADA system is measured by the ratio *loss of load/total load* through power flow simulation. Experiments are conducted on a case study via simulation of the power flow and dynamic analysis. The integration of the cyber and power models is based on the simplifying assumption that cyber attacks can provoke unexpected opening of circuit breakers and the associated loss of electric load.

The assessment of *survivability* of a network with virtual connections exposed to node failures is discussed in [424]. Survivability modeling assumes that an undesired event already has occurred and therefore the frequency of such an event is dispensable. Survivability models objective is to quantify the level of service degradation during system recovery periods. Both a time-space decomposed analysis based on continuous time Markov chains (CTMCs) and a simulative approach have been used to cross validate. A number of scenarios with different network sizes have then been analyzed with respect to the survivability of the network.

Testbeds are used to conduct empirical studies of resilience assessment. A security testbed [753] has been built to emulate a SCADA network that is going through a Denial of Service (DoS) attack. Several national and international collaborative approaches for testbed implementations exist [212]. Testbeds have also been developed and evaluated as part of ongoing research programs on critical infrastructures, such as CRUTIAL [112, 247] and IRRIIS [470].

Network theory and graph-based representations of the infrastructures' topology are often applied to study interdependencies and relevant properties of the structure of a system. Such representations can be used for both qualitative and quantitative approaches.

The focus of [28] is on data survivability in pipeline systems. Two weighted graphs are constructed, one representing the pipeline structure and the other representing the set of sensors and their interconnections. Different types of constraints have to be respected such as source/sink balance, flow conservation, maximum bandwidth, and the availability of energy. The optimal network topology problem is solved using known algorithms for the solution of the Maximum Concurrent Multicommodity Flow problem.

In [863] a *graph-based* approach is used in combination with *statistical analysis*. Directed multigraphs augmented by response functions represent the interactions between the network components, and are used to analyze the interdependent effects of random failures and targeted attacks. Graph elements exist for non-storable resources (e.g., in the electric grid network), storable resources (e.g., in gas or oil pipeline), reliability (e.g., in the telephony transport layer), types of failures, repair time, and logistic delay. Graph statistics and analytical approaches are used to identify critical components. The simulation experiments show that a failure in the gas

distribution network leads to a total failure in the telecommunication network and to reduced functionality of the power distribution network.

The authors of [126] conduct a *structural analysis* of the power transmission grid by applying a topological approach that extends the traditional metrics derived from complex network theory (e.g., degrees of nodes and global efficiency) with two new metrics, the entropic degree and net-ability. The new metrics account for the physical and operational behavior of power grids in terms of real power-flow allocation over lines and line flow limits. This approach can be used to assess structural vulnerabilities in power systems in contrast to traditional, purely topological metrics. The impact analysis of control systems availability on managing power contingencies is not supported by this extended topological approach.

More techniques to cope with CI models naturally exist, such as agent-based [882] and Monte-Carlo simulation approaches [115, 788]. High Level Architecture (HLA) or spatial reasoning using GIS [557] can be applied to distributed simulation. Exhaustive methods such as model-checking or performance evaluation approaches can also be applied. Multiformalism modeling [340] incorporates different modeling formalisms and applies dedicated solvers to obtain results in heterogeneous environments.

3.3.3 Current Programs

There are a number of ongoing projects in the field of critical infrastructures that mainly focus on quantitative analysis and interdependency analysis of the power grid using simulation models. For example, Trustworthy Cyber-Infrastructure for Power (TCIP) [868, 869] models trust and security issues for power and SCADA systems. Placing SCADA data communication on the Internet creates an environment where providing a reliable computing base is a challenge. Therefore, TCIP connects simulation models and tools developed for the power grid with those developed for the internet. Quantitative and qualitative evaluation constitute major research efforts in TCIP [801], with focus on means to model, simulate, emulate, and experiment with the various subsystems in the power grid. A variety of evaluation tools are adopted to enable validation, including PowerWorld, RINSE, formal logic, PowerWeb and APT.

In the CRitical UTility InfrastructurAL resilience (CRUTIAL) project [112, 247], the emphasis lies on ICT infrastructures for electric power grids, the study of interdependencies and the analysis of critical scenarios. The Integrated Risk Reduction for Information Based Infrastructure Systems (IRRIIS) project [470] focuses on simulation approaches, with emphasis on interdependencies in information-based infrastructure systems. Both projects focus on the analysis of interdependencies and will be discussed in more detail in Sect. 3.4.

Vital Infrastructure Threats and Assurance (VITA) [747] aims to raise awareness to the vulnerabilities of critical infrastructures by creating simulations and using role-plays. The project developed methods, tools and techniques for infrastructure

protection and a demonstrator experiment with a focus on energy that can be used to gain insight into protection mechanisms on an international level.

The focus of the reliable infrastructures sub-project of the Next Generation Infrastructures project [745] is on the design approach for damage prevention to infrastructures and on the avoidance of system instabilities in the presence of failures. For example, the research on distribution centers security aims at ensuring the survivability of vital nodes in a networked information infrastructure to prevent system-wide failures. Another goal of the research is the protection of integrated ICT departments.

The Power Systems Engineering Research Center (PSERC) [746] does research on power markets, power systems, transmission and distribution technologies. This research aims at increasing the efficiency and reliability of increasingly complex and dynamic power systems through modeling, evaluation, and control. One area of research is the development of estimation techniques that use past system-wide failure data to help in the prediction of future system-wide failure events.

3.4 Focus on Interdependencies Modeling and Analysis

As already discussed in Sect. 3.2.1, strong dependencies exist among infrastructures, which can easily become a vehicle through which faults, errors and attacks propagate. If not controlled, these dependencies can create a multiplicative effect, leading to cascading and escalating failures of one or more critical infrastructures. It is thus extremely important to understand the associated relationships, for the prevention and limitation of threats and vulnerability propagation, and for recovery and continuity in critical scenarios.

Among the most recent efforts in addressing the modeling and analysis of interdependencies in critical infrastructures, we briefly recall the activities developed in the context of the European initiatives IRRIIS [740] and CRUTIAL [245], and some other works from the literature.

3.4.1 The CRUTIAL Approach

The CRUTIAL project [245] has addressed new networked systems based on ICT for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intra-nets) that are in turn connected to the Internet.

The project has developed new architectural patterns that are resilient to both accidental failures and malicious attacks, and comprehensive modelling approaches, supported by measurement based experiments, to analyse critical scenarios in which

faults in the information infrastructure provoke a serious impact on the controlled electric power infrastructure.

In CRUTIAL the interdependencies between infrastructures have been investigated by means of models at different abstraction levels: (i) from a very abstract view expressing the essence of the typical phenomena due to the presence of interdependencies, (ii) to an intermediate level of detail representing in a rather abstract way the structure of the infrastructures, in some scenarios of interest, (iii) to a quite detailed level where the system components and their interactions are investigated at a finer grain, considering elementary events occurring at the components level and analyzing their impact at the system level. Accordingly, the proposed framework is based on a hierarchical modelling approach that accommodates the composition of different types of models and formalisms, including generalized stochastic Petri nets (GSPNs), fault trees (FT), Stochastic Well formed Nets (SWN), and Stochastic Activity Networks (SAN). Each of these formalisms brings particular benefits that motivated its selection into the CRUTIAL modelling approach. However, this choice is not exclusive, and other formalisms with equivalent characteristics could also be used. Significant contributions have been obtained by CRUTIAL considering the qualitative description of interdependencies related-failures (mainly, unified models considering accidental and malicious threats in a integrated way) and the quantitative assessment of their impacts on the dependability and security of electrical power systems services [247].

The approach has coped with the lack of data representing realistic probability estimates of the occurrence of cyber threats and consequent failure modes by creating two complementary testbeds. These have been set up to run controlled experiments and to collect otherwise unavailable data related to cyber misbehaviours on grid teleoperation and micro grid control scenarios. One platform, the telecontrol testbed, consisted of power station controllers on a real-time control network, interconnected to corporate and control centre networks. The other platform, the microgrid testbed, was based on power electronic converters controlled from PCs, interconnected over an open communication network. Both testbeds integrated elements from the electrical infrastructure as well as from the ICT infrastructure, in order to focus on their interdependencies, and specifically on the vulnerabilities that occur in the electric power system when a part of the information infrastructure breaks down [248].

3.4.2 The IRRIIS Approach

The IRRIIS project [470] aims at increasing dependability, survivability and resilience of EU ICT-based critical information infrastructures. The basis for this work is the knowledge elicitation focused on interdependencies between the two infrastructures “electricity” and “telecommunication including Internet”. Several approaches have been pursued to model and analyze the interdependencies.

A theoretical framework has been developed in [689], where an approach equivalent to process modeling is adopted, which views a CI as a process and dependencies

that are modeled as response functions. Quantitative interdependency analysis, in the context of large complex critical infrastructures, is presented in [115], where a discrete state-space continuous-time stochastic process is used to model the operation of the critical infrastructure, taking interdependencies into account. Of primary interest to the model are the implications of the level of abstraction and parameterization for the study of dependencies on the distribution of cascade-sizes within and across infrastructures. The Leontief input-output economical model representing market dynamics has been exploited and adapted to model critical infrastructures dependencies [471]. In addition, an empirical approach [612] has been applied to analyse a large set of critical infrastructures failure data to discover patterns across infrastructures failures.

The IRRIIS consortium has developed Simulation for Critical Infrastructure Protection (SimCIP), an agent-based simulation environment for controlled experimentation with a special focus on CIs interdependencies [536]. The simulator is intended to be used to deepen the understanding of critical infrastructures and their interdependencies and to identify possible problems. It is intended to be used to validate and test architectural solutions aiming at enhancing the dependability of large critical information infrastructures. The network model for SimCIP is based on a multi-layer simulation approach (technical, cyber, management).

3.4.3 Other Studies

In addition to the work reported in the previous sections, several other simulation models have been proposed to analyze interdependencies, in the context of Electric Power Systems [42, 190] and in connection with telecommunication networks [42, 282, 782, 787]. A study to identify the state-of-the-art in critical infrastructures interdependency modelling and analysis and the government/industry requirements for related tools and services has been described in [116], where a strategy aiming to bridge the gaps between existing capabilities and UK government/industry requirements is also presented. In the report [720], the field of infrastructure interdependency analysis is first presented, then a survey on modeling and simulation techniques used for the infrastructure and interdependencies is introduced together with the leading research efforts. Data was collected from open source material and when possible through direct contact with the individuals leading the research. The issue of identifying appropriate metrics for quantifying the strength of interdependencies has also been addressed in a few studies, such as [177, 791].

3.5 Focus on Fluid Infrastructures

Since different infrastructures have different characteristics, this section provides a survey of the modeling requirements for so-called *fluid critical infrastructures*, i.e.,

water, gas and oil treatment and distribution. In contrast to e.g., power transmission and distribution networks, fluid infrastructures have mainly linear characteristics and as opposed to power, the fluid can be easily stored. Taking these specifics into account, it is possible to come up with a suitable and scalable modeling formalism and analysis technique for fluid infrastructures, as presented in [393] and summarized below.

A recent report of TNO Defence and Security [610] analyzes the current situation in the water sector and found a large number of vulnerabilities. Based on this research a number of detailed measures have been proposed [611] to increase security in the water sector. Given the severe consequences of successful attacks on SCADA systems, it is very important to analyze the trade-off between the cost and the efficiency of such measures, already in the design process. The efficiency of these measures can be expressed in terms of survivability, i.e., the time it takes after a successful attack, before the system recovers to an acceptable level of service.

An example critical infrastructure that intensively uses SCADA systems for process control are wastewater-management systems. Water is cleaned in several chemical and physical cleaning steps, before it is distributed to the end users. A suitable modeling formalism for such systems needs to take into account continuous and discrete quantities, as well as random failure and repair times. SHMs combine discrete and continuous variables with stochastics, hence, allow to model random phenomena in a natural way. On the one hand, a very nice theory has been developed that takes into account the full expressiveness of Stochastic Hybrid Models [737]. However, the industrial application that we are considering is by far too large for state-of-the-art approaches; hence the focus of the presented approach is on scalability. On the other hand, several formalisms supporting SHMs have been defined [263, 395, 444], where each of them is suitable only in some very specific domain, and suffers from limitations that prevent it from being used in other applications.

Recall, that interdependencies between the physical process and the ICT control infrastructure are crucial in critical infrastructures. Therefore critical infrastructures are very big and complex systems and scalability is of utmost importance. State-of-the-art analysis methods from the area of SHM, however, do not scale. The systems under consideration are characterized by deterministic fluid transportation, however, with rates that change according to a stochastic process. Hence, Fluid Stochastic Petri Nets (FSPNs) [395, 444] and Piece-wise Deterministic Markov Processes (PDMPs) [263] appear to be suitable. However, the memory of continuous variables in PDMPs is lost upon stochastic transitions. Hence, they are not suitable to model the physical behaviour of fluid critical infrastructures. First and second order Fluid stochastic Petri nets (FSPNs) [395, 444] have a sound mathematical basis allowing for a completely formalized characterization of the state-evolution in terms of differential equations. However, such equations can be solved only when there are at most one or two continuous variables. Simulation is the only available alternative when considering larger models [221, 394]. Another limitation of current FSPN approaches is the lack of efficient compositional techniques.

The above clearly shows the need for a modeling and analysis framework that is specifically tailored towards fluid critical infrastructures. To tackle the issue of

scalability, a new approach based on Hybrid Petri nets [261] was proposed, where the deterministic evolution is separated from the stochastic behaviour of the system [393], by exploiting the quasi-deterministic behaviour of the system under study, given that failure and repair events are stochastic. Therefore, there are relatively few stochastic transitions, which allows for separating the deterministic and the stochastic evolution of the system, using a conditioning/deconditioning argument. This will speed up the reachability analysis and will allow for a large number of continuous variables in the model, as opposed to previous approaches.

The Hybrid Petri Net formalism with General one-shot transitions (HPNG) as proposed in [393] is specifically tailored towards fluid critical infrastructures. It allows for an arbitrary number of continuous variables that can be connected via fluid transitions. These transitions can be controlled by discrete places that can be connected via deterministic and generally distributed transitions. Generally distributed transitions must respect the constraint that they can fire only once during the evolution of the model: for this reason we call them one-shot transitions.

Gribaudo and Remke [393] also introduces a new and efficient computation scheme for all reachable states of a model: parametric reachability analysis. This technique separates the deterministic and the stochastic components of a HPNG by conditioning the deterministic evolution on the samples drawn from the probability distributions associated to the general transitions. After all reachable parametric locations have been computed, important performance metrics (such as the distribution of fluid) can be derived by a deconditioning procedure. As opposed to similar SHM solution algorithms, the presented technique allows for an arbitrary number of fluid variables.

The algorithm as described in [393] presents a first step in the analysis of HPNGs and needs to be extended in several ways to realistically model and analyze fluid critical infrastructures. Currently, the algorithm only allows for one general one-shot transition, resulting in an underlying state-space of parametric locations that depend on the sample of the one general transition. The approach used can be made more scalable by extending the algorithm to allow for more generally distributed transitions resulting in parametric locations that depend on as many samples.

In [393] the effect of different failure and different repair time distributions is shown for a model of a water treatment facility. Possible results include the distribution of fluid during the recovery process and the probability to reach an unsafe state after a failure or attack. This helps system engineers to dimension storage tanks in a way that failures do not influence the continuity of water delivery. In industry, there is currently a trend towards combining the processing of drinking, surface and waste water into one integrated water network, which makes the system even more complex and hence, more vulnerable. Moreover, due to legal constraints in the Netherlands, by 2014 the operation of the water treatment and distribution has to be fully automated without direct human control. This requires the a priori development of optimal repair strategies. Hence, water companies are very interested in evaluating the dependability of their infrastructures and in comparing design alternatives based on a cost/benefit analysis.

3.6 Case Study: Reliability Modeling of a Smart-Grid Distributed Automation Network

This section illustrates a reliability assessment approach for a distributed automation Smart-Grid network. Specifically, we present the computation of the System Average Interruption Duration Index (SAIDI) metric for one specific power distribution circuit, which consists of 7200 feet of the main distribution line, encompassing 117 transformers and serving a total of 780 customers [931].

SAIDI is one of the most important performance metric for power utilities, as it evaluates the utilities' performance after a sustained power interruption. For example, SAIDI is used in the United States by public service commissions to monitor and control power utilities performance.

Some regions in the United States determine utility power rates based on the utility performance as measured by SAIDI and other metrics that are related to the time to restore power after a failure event and the number of customers affected by a power failure. Therefore, utilities are required to measure and report SAIDI to the controlling public service commissions. The public service commission has the power to investigate failure events and to order the power utility to improve performance [930].

The main circuit line is equipped with a distributed generator system at the end of the line that can be switched on when faults are detected on the main line or to provide an additional source of load. The peak load of the main line is 1692 KW, measured in August, i.e., during a hot midweek summer day. The distributed generator is designed to provide 100 % of the circuit load, i.e 1692 KW. The distribution network is composed of 34 feeder lines that are connected to the main circuit feeder. Figure 3.3 shows one feeder line divided into 40 sections. The back-up generator connects to the main feeder line through a Tie switch, not shown in Fig. 3.3. Each main feeder line can be divided into several sections, at a significant cost for construction and maintenance per section. The added benefit of increased number of sections is the increased level of granularity of power control.

Currently, the main feeder line is not divided into sections, so if a fault occurs on the main line, all the customers on the main feeder line would be impacted. The objective of implementing a Smart-Grid distributed automation approach is to decrease the customer impact of power failure events as assessed by the expected value to the SAIDI metric.

In a distributed automation approach, after a power failure event, the faulty section is switched off the main line, and the substation powers the upstream part of the feeder, while the distributed generator powers the downstream part of the feeder, reducing the outage impact only to the customers that are supported by the now isolated failed section. Therefore, while the customers in the faulty section still see an outage with an average repair time of 4 h, the other customers that are served by the main feeder line, experience a power interruption that will last only about 2 min. The tradeoff in this distributed automation design is the cost and complexity of having many

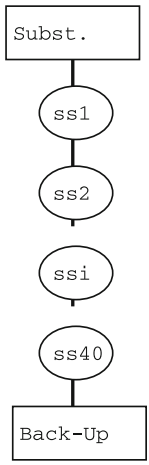


Fig. 3.3 Architecture model of one main feeder line divided into 40 sections

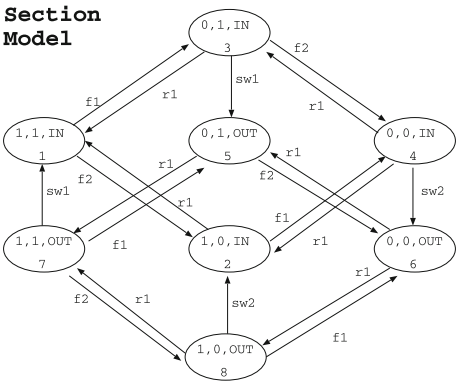
sections, against the large customer impact of the failure of a large section, if too few circuit sections are implemented.

In this example we use hours as the unit for the failures and repair rates. SAIDI is defined as $\sum(r_i \cdot N_i)/N_T$, where r_i is the actual service restoration time in hours, N_i is the total number of customer interrupted, and N_T is the total number of customers [930].

Figure 3.4 presents a Markov reward model of the states a given section can be in, due to failures, repairs, and section line switches, that are needed to isolate the failed section from the main circuit feeder line. Each state is described by a three tuple, where the first entry captures the power state (on/off), the second entry represents the state of the smart-grid communications network (on/off), and the third entry characterizes whether the section is currently in-line or out-of-line.

When the distributed automated network is operating correctly, the Markov chain is in state $s = (1, 1, IN)$, which is state 1 in Fig. 3.4. We have to consider two different types of failures:

- A power failure with impact on the section under study occurs with rate f1 and the Markov chain will transition to state $s = (0, 1, IN)$. The power failure has to be repaired in stages. If the smart-grid automated repair is functioning properly, the Markov chain moves to state $s = (0, 1, IN)$, after the power failure. Next, the Markov chain moves with rate sw1 to state $s = (0, 1, OUT)$, where the section is removed from the line. In this state all customers upwards and downwards from the failed section already have their service restored. Typically, the average time to switch a section off-line is between 1 and 2 min. The average time to repair a power failure manually is between 1 and 4 h, depending on several factors like, urban density, traffic congestion, cause of equipment failure, and the extent of the damage to the equipment [736]. In this example, we assume the average switching




```
State = (Energy, Network, Line)

Transition Rates

f1 = 0.000000627 power fail/hour
f2 = 0.00005     network fail/hour
r1 = 0.25        repair rate/hour
sw1= 30          network switch rate/hour
sw2 = 1          manual switch rate/hour
```

Fig. 3.4 Markov reward model, describing failures and repairs in a distributed automation power network

time, $1/sw1$, to be equal to 2 min, and the average manual power failure repair time,$1/r1$ to be equal to 4 h. When the power failure is corrected manually, the Markov chain moves to state $s = (1, 1, OUT)$, with rate r1 and from this state the section is switched back on with rate sw1. Then, the customers from the affected section have their power restored.

- A smart-grid failure occurs with rate f2 and which impacts the section under study, the Markov chain will transition to state $s = (1, 0, IN)$. In this state there is no impact on the power-grid service to the power customers. However, if a power failure occurs in this state, with rate f1, the Markov chain moves to state $s = (0, 0, IN)$. In this state all customers in the main feeder line suffer from the power failure and the line has to be manually switched off, with rate sw2, to isolate the section from the main feeder line. From state $s = (0, 0, OUT)$ a manual repair brings the Markov chain to state $s = (1, 0, OUT)$ and a manual smart-grid repair brings the Markov chain to state $s = (1, 0, IN)$. In this state the power is restored for all customers but the automated Smart-grid recovery is still not repaired. When the Smart-Grid is repaired the Markov chain moves to the initial state $s = (1, 1, IN)$. The other transitions follow a similar pattern and are shown in Fig. 3.4.

One of the challenges in Reliability modeling is the expression of the system reliability degradation as a function of time, which is often overlooked. Therefore, we solved the Markov chain model with rewards using the Tangram-II [272] transient analysis solver. A Markov chain with rewards analysis was used to represent one year of operation. The model captures only one section failure at a time. Therefore, an important assumption used in this Markov modeling example is that the smart-grid is designed to automatically restore one section failure at a time, and that the probability of occurrence of a second power failure while the first one is being repaired is very small.

Table 3.1 SAIDI after 1 year of operations for several section designs, for 0.1 power failures/km/year and 1/20, 000 failures per hour communications network equipment, manual repair time of 4 h, automated section switching time of 2 min, manual line switching of 1 h, total number of customers served by main feeder line equal to 780

Number of sections	Customers impacted	f1	f2	SAIDI
5	156	0.000005	0.00005	0.036
20	39	0.000001252	0.00005	0.0025
40	20	0.000000627	0.00005	0.00074

Table 3.1 presents the computed SAIDI metric for different alternatives of section designs after one year of operation. These results are derived from the solution of a transient Markov reward model for a section failure rate of 0.1 failures per km per year. This analysis is useful for the engineering of the topology of distribution automation networks, where the engineer needs to tradeoff between the investment in number of sections and the distribution automation reliability.

The empirical results shown in Table 3.1 illustrate the tradeoff between increased reliability and the additional cost of designing a larger number of sections into the main feeder line. Table 3.1 shows that to achieve increased reliability a larger number of sections has to be built, at additional cost for construction and maintenance. The benefit obtained from the construction of sections that control a smaller number of users that can be isolated quickly in the case of power failures is the improved power reliability, which is demonstrated by the smaller values of the SAIDI metrics for the main line feeder design when the feeder line is divided into 40 sections.

3.7 Conclusions and Emerging Research Directions

Following the more comprehensive approach of CI resilience as presented in [677], state of the art resilience assessment approaches for CIs should help improve the robustness of CIs. The increase in robustness of CIs can be achieved by increasing their absorptive capacity, their resourcefulness or their recoverability. The absorptive capacity, for example, can be improved by adding more redundancy. Resourcefulness is the ability of using the available resources efficiently in the presence of failures and disasters. It depends mainly on the adaptive capacity of the system. Optimized repair schedules can improve the resourcefulness of critical infrastructures. Finally, recoverability can be optimized by minimizing repair times. On one hand, improvements to the robustness of critical infrastructures come at a certain cost. On the other hand increased robustness will reduce costs due to systems down time. Hence, the resilience of critical infrastructures should be evaluated under a cost-minimization criteria.

The variety of initiatives in resilience assessment of critical infrastructures, some of which are briefly overviewed in this chapter, testify to the paramount role of

resilience assessment in several critical sectors. However, when comparing requirements for resilience assessment, as identified in Sect. 3.2, with existing approaches, as discussed in Sect. 3.3, it becomes clear that further research is still required. Most of the modeling research in CIs uses simple handcrafted reliability block diagrams, fault-trees, or simplistic stochastic Petri nets. Recent research on fluid critical infrastructures suggests that stochastic hybrid systems can be tailored toward this new application field. The application of stochastic methods captures the continuous dynamics of the physical world and the discrete characteristics of the control infrastructure. However, further research is necessary to ensure the scalability of hybrid approaches.

Advances in industrial control systems and technology, such as SCADA systems, enhance sector operations but create additional vulnerabilities and increase interdependencies, whose effects are hard to detect and to mitigate. To make these systems resilient, research must integrate an understanding of resilience, security, human interaction, and complex network design to address the threats. The largeness and diversity of critical infrastructures and the different characteristics of their parts requires a compositional integrated formalism. The necessity of continuous assessment activities calls for a composite (i.e., holistic) evaluation framework, where the synergies and complementaries among several evaluation methods can be fruitfully exploited.

Further research is required to develop coherent resilience properties in different sectors of CIs. Sound and rigorous definitions of measures, such as recoverability and survivability, can be cast into temporal logics, e.g., continuous stochastic logic [228]. Research into recently developed methods for stochastic model checking needs to be adapted for the use within critical infrastructures. The use of abstraction, bi-simulation reduction, and symbolic state space representation techniques can help to tackle large state-spaces. In addition, the use of simulation-based statistical model checking can be a applied to the assessment of resilience of CIs.