Chapter 2
Modelling Dependencies Between Critical Infrastructures

Roberto Setola and Marianthi Theocharidou

Abstract This chapter provides an overview about dependencies among infrastructures and discusses how they can be adequately captured, modelled and analyzed. It provides a taxonomy overview of the most adopted methods with a focus on the IIM (Input-output Inoperability Model) and on topological approaches.

1 Introduction

Dependencies among infrastructures are usually complex and non-obvious. They may allow cascading disruptions or failures to different infrastructures, thus causing a potentially significant impact to multiple types of sectors, individuals or countries. Well-known examples of such cascading effects include the electric power disruptions in California in 2001 [1], as well as the major blackouts in the USA, Canada and Europe in 2003 [2].

Identifying CI dependencies leads to a more accurate assessment on the criticality level of a single infrastructure element, or even of a whole sector. It also enables the identification of dependency chains among dependent CIs. In this way it becomes possible to identify the 'most' critical among the infrastructures and adopt more cost-efficient security controls, so as to reduce overall risk [3]. The identification of such dependencies is also important during the risk assessment and planning phase so as to ensure that the mitigation and the recovery processes take into account such relationships among infrastructures. Recently, dependency models are increasingly

R. Setola (✉)
University Campus Bio-medico of Rome, via A. del Portillo 21,
00128 Rome, Italy
e-mail: r.setola@unicampus.it

M. Theocharidou
European Commission, Joint Research Centre, via E. Fermi, 2749,
21027 Ispra, VA, Italy
e-mail: marianthi.theocharidou@jrc.ec.europa.eu

© The Author(s) 2016

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_2

used to support emergency managers in order to better prepare and plan for possible cascading effects [4].

This chapter provides an overview about the types of dependencies that can be observed among infrastructures. It also analyses the different approaches which are currently applied for modeling, with a focus on the IIM (Input-output Inoperability Model) and on network based approaches. These approaches were selected because of their comprehensiveness; indeed due to their simplicity they can be a starting point when studying modeling for Cls (see also Chap. 6 for more information on the topic).

2 Why Are Dependencies Important?

The well-known electric failure scenario of California [1] is an illustrative, real case of complex and multi-order dependency. The electric power disruptions in California caused cross-sectoral cascading consequences, affecting the natural gas production, the operation of petroleum product pipelines transporting gasoline and jet fuel within California, Nevada and Arizona, and the operation of massive pumps used to move water to crop irrigation (*first-order dependencies*). Gas production curtailed by power losses directly impacted gas supplies for generating units, further exacerbating power problems (*feedback loop*). Tight natural gas supplies also had the capability to shut down gas-fired industrial co-generation units producing steam to be injected into California's heavy oil fields (*second-order dependencies*), thus potentially reducing heavy oil recovery (*third-order dependencies*). Similarly, the disruption of pipelines caused inventories to build up at refineries and draw down at the product terminals (*second-order dependencies*), including several major Californian airports. Declining jet fuel stocks at airports entailed several major airline operators to consider contingency plans in the case of fuel shortages (*third-order dependencies*).

In the same way, the blackouts in the USA-Canada (August 2003), Southern Sweden and Eastern Denmark (September 2003) and Italy (September 2003) highlight the possibility of international cascading effects. These examples depict how a single event or incident occurred in one infrastructure, whose effect may have been assessed to cover a (geographically or sectoral) limited number of entities, is in fact affecting many other CIs. In all three blackouts, we observe a chain of failures causing cross-border effects and a significant impact to people.

The impact of a disruption, or failure, may spread both geographically and across multiple sectors. Identifying dependencies is therefore an important task. However, in many cases special types of dependencies are not obvious and easy to identify. For example, socially derived or human-initiated dependencies may refer to changes in behavior of individuals, which can be observed during a crisis. Such changes in behavior may consequently affect infrastructures or networks in a different way than the one initially perceived. A disruption in the transportation sector may cascade to wireless communication networks [5], due to alterations on calling

patterns and activities, which may affect the load on wireless networks and cause disruptions in communication.

Although the identification of first-order interdependencies may be sufficient, in order to assess the risk of a particular CI, they may fail to capture cascading effects at a macroscopic level. For example, one or more, relatively minor, incidents on one CI may cause cascading and escalating impacts to a dependent CI of a second or third level. Even worse, a second or third-level effect may in turn affect the initiating source of the problem and in this way cause a feedback effect, which will further increase the total impact of the incident.

The identification is even more complex due to the fact that dependencies may also shift on the mode of operation of the CI [6]. An example of this shift in dependency, is that in case of power loss, a hospital is dependent on diesel fuel when running on emergency power.

3 Dependencies and Interdependencies

In the literature several definitions of "dependency" and "interdependency" were presents; however one of the most widely accepted is [7]:

Dependency is the capability of an infrastructure to influence the state of other infrastructures. Then infrastructure A depends on infrastructure B when a variation in this latter has the capability to influence (e.g. modify) some states (e.g., behaviours, characteristics, properties, etc.) of infrastructure A. It is, therefore, a unidirectional relationship.

Dependencies between two infrastructures (or their functions/services) may be direct or indirect (see Fig. 1). Infrastructure C may be directly dependent on infrastructure A (**direct dependency**), or dependent of infrastructure B (or a recursively a chain of infrastructures) which in turn is dependent on infrastructure A (**indirect dependency** C of A). Notice that in this last case we indicate that B has a second order dependency on A, i.e. the number of "hop" in the dependency chain represent the order of dependency.

On the other side the term **interdependency** represents a bidirectional relationship between two or more infrastructures where the state of each infrastructure is influenced or is correlated to the state of the other. Hence, infrastructures A and B are interdependent if A depends on B and, at the same time, B depends on A, As shown in Fig. 1, such bi-directional dependency can be mediated by other infrastructures.

Notice that the presence of interdependency creates loops of reciprocal influence. In the presence of loops the consequence of any fault it can no longer be described via described via a tree structure (where there is a root and the consequences go only downstairs) although the propagation has a graph structure, i.e. the consequences have no preferential direction. This implies that negative consequences in any infrastructure are exacerbated.

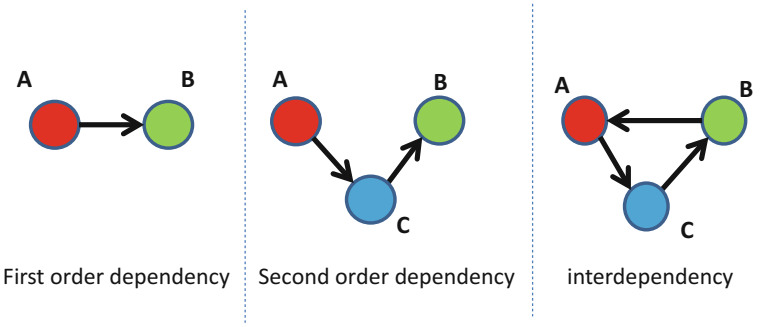

Fig. 1 Dependency and interdependency

In the framework of Critical Infrastructure Protection (CIP), we generally limit our attention only on the phenomena strictly related to services and functionalities degradation. In other terms, we consider a steady-state configuration for the overall system and we characterise dependencies and interdependencies on the basis of the effect that a failure (accidental event or malicious attack) in a component/infrastructure induces on the other elements in terms of worsening degradation of their functionalities.

Going further into detail in [1] it is emphasised that interdependencies should be analysed with respect to six different dimensions, which include characteristics of the infrastructures, of the environment, the type of failure, the operative condition and the phenomena that generate the coupling. In particular, they catalogue such phenomena into four not mutually exclusive classes:

- *Physical interdependency*—Two infrastructures are physically interdependent if the operations of one infrastructure depend on the physical output(s) of the other.
- *Cyber (inter)dependency*—An infrastructure presents a cyber-interdependency if its state depends on information transmitted through the information infrastructure.
- *Geographical (inter)dependency*—A geographical interdependency occurs when elements of multiple infrastructures are in close spatial proximity. In this case, particular events, such as an explosion or a fire in an element of an infrastructure, may create failures in one or more infrastructures in close proximity.
- *Logical (inter)dependency*—Two infrastructures are logically interdependent if the state of each one depends on the state of the other via control, regulatory or other mechanisms that cannot be considered physical, geographical or cyber.

In addition in [8] an additional category of dependencies is introduced:

- *Social dependency.* The link between the CIs is based on impacts caused by human behaviour. For example, the state of a CI is affected by the spreading of disorder to another CI related to human activities. This models the (irrational)

human behaviors in the case of crisis, e.g. overloading communication system or collective panic reactions.

In [1] it is stressed that cyber interdependency tends to become an absolute and global characteristic of all the infrastructures, while other types of interdependencies are more local. Cyber dependency potentially couples an infrastructure with every other infrastructure that uses the cyberspace, in spite of their nature, type or geographical location.

A different, but similar, classification can be found in [9] where the authors consider: Physical, Geospatial, Policy, and Informational.

Using a dataset on CI disruption incidents, empirical analysis [10, 11] showed that interdependencies—mutual dependencies—seldomly occur. Newer analysis shows that the only interdependencies that are mentioned in press reports occur at a lower, component or subsystem, level of abstraction. No 'shooting in one's own foot' has been observed where A depends on B, B on A, and the disruption of A causes B to get disrupted causing A not being able to recover at all as B's critical functions are disrupted.

Using this understanding, Nieuwenhuijs et al. [6] concluded that the set of 'interdependencies' presented by Rinaldi et al. on 2001 needed a reassessment. They stated that the geographical interdependencies are not dependencies but they are the result of a **common mode failure** (e.g. astorm) and that the mentioned 'interdependencies' are just 'dependencies'. Dependencies are not a binary on/off phenomenon but shall be seen as the service level of quality (or set of qualities), e.g. the triple pressure, biological purity, and chemical purity of drinking water. Only when the service level drops below the expected service level, a dependency may cause a 'cascading' disruption in the dependent function, service, or infrastructure. The degradation and recovery characteristics for each quality are infrastructure specific functions, such as the slow loss of pressure in drinking water pipelines after the failure of the distribution grid pumps amplified by on-going demand, and the slow system recovery as repressuring takes time. Their analysis also shows that those who analyze CI dependencies also need to take into account the **mode of operation**. The daily set of dependencies (normal operations) may be very different from the set of dependencies when a CI has been disrupted (stress mode of operation), the dependencies in the crisis mode of operation, and during the recovery. For instance, a hospital is not dependent on diesel fuel, diesel trucks, truck drivers and lumbermen for their normal operations. But when a big storm hits and downs power lines, the backup generator starts. When the diesel tank starts to run dry, the hospital needs to order diesel, requires diesel transport (fuel loading, truck, driver) and a road cleared from toppled trees. Alike, for recovery, one may need an extraordinary large crane to repair critical infrastructure. To identify such sets of shifting dependencies it is required the analysis of the scenarios beyond the analysis of a disruption of a single CI.

In [12], it is emphasised that, to correctly understand the behaviour of these infrastructures, it is mandatory to adopt a three-layer model:

- *Physical layer*—the physical component of the infrastructure, e.g., the grid for the electrical network.
- *Cyber layer*—hardware and software components of the system devoted to control and to manage the infrastructure, e.g., SCADA and DCS.
- *Organisational layer*—procedures and functions used to define activities of human operators and to support cooperation among infrastructures.

Here, the authors emphasise that each component of an infrastructure interacts, further than the other components of its infrastructure in the same layer also with the components of its infrastructure posed in the other layers (by means of internal links indicated as "inter-dependency"). Moreover, any component also interact with elements in the same physical/cyber/organizational layers of other infrastructures, by means of external links denoted as "extra-dependency". The increasing presence of these latter links creates many functional dependencies among infrastructures. Moreover, the authors emphasise that, with respect to ten years ago, the importance of the cyber layer is largely increased, becoming one of the most important sources of interdependencies. Notice that a similar kind of decomposition was also used to analyse the 2003 blackout in the USA and in Canada [13]. As a matter of fact, to explain the multitude of causes that produced that episode, the joint of USA and Canada governmental investigative commission described the event in terms of grid (physical), computer and human layers. Only by considering all the layers together it is possible to correctly understand what really led to the blackout.

The dependence-related disruptions or outages have also been classified as *cascading*, *escalating* or *common-cause* [1]:

- A cascading failure is defined as a failure in which a disruption in an infrastructure A affects one or more components in another infrastructure, say B, which in turn leads to the partial or total unavailability of B.
- An escalating failure is defined as a failure in which an existing disruption in one infrastructure exacerbates an independent disruption of another infrastructure, usually in the form of increasing the severity or the time for recovery or restoration of the second failure.
- A common-cause failure occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause. This occurs when two infrastructures are co-located (geographic interdependency) or because the root cause of the failure is widespread (e.g., a natural or a man-made disaster).

A more recent empirical study [11], shows that events can been classified as *cascade initiating* (i.e., an event that causes an event in another CI), cascade resulting (i.e., an event that results from an event in another CI), and independent (i.e., an event that is neither a cascade initiating nor a cascade resulting event). The empirical findings indicate that:

1. cascade resulting events are more frequent than generally believed, and that cascade initiators are about half as frequent.
2. the dependencies are more focused and directional than often thought.
3. energy and telecommunication are the main cascading initiating sectors.

Luiijf et al. [14] also argue that most current dependency models neglect to recognize multiple states of operation. They usually focus on identifying dependencies under normal operational conditions, failing to model the dependencies that may emerge as soon as the operation of an infrastructure deviates from these conditions. They highlight that cascading failures may occur due to CI operators not realizing that they face different sets of dependencies in each operational state. To this end, they identify four different states of CI operation to be considered when performing dependency modeling:

- *Normal*: the state in which a CI operates under normal operational conditions.
- *Stressed*: state in which a CI operates when special measures have to be taken to keep the operation under control.
- *Crisis*: this is the state where the operation is out of control.
- *Recovery*: this is the state where the operation is again brought under control but has not yet been restored to the normal state.

A related work in identifying and modeling dependencies includes the use of sector-specific methods, e.g., gas lines, electric grid or ICT, or more general methods that are applicable in various types of CIs. In the following section, we review and illustrate some of the most popular methods to model dependencies phenomena.

4 Dependency Modeling Approaches

As noted in [1] the relevance, mechanism and effect of the dependency varies according to geographical scope under analysis. Generally more large is the area of reference, more relevant are the phenomena induced by the presence of (inter) dependencies.

Different approaches have been used to examine dependencies under a microscopic or macroscopic point of view. De Porcellinis et al. [8] refer to reductionistic and holistic approaches. A reductionistic approach identifies elementary components within a CI and then describes the evolution of the entire system based on the aggregated behaviour of these components. Holistic examples include the study dependencies between different CIs [6], within the same or different sectors of a country [15]. Many holistic approaches apply Leontief's inoperability input-output model (IIM), which calculates economic loss due to unavailability on different CI sectors based on their interdependencies.

In the literature, a uniform data collection method has not been implemented, which means that a significant effort needs to be placed to sort, evaluate or combine

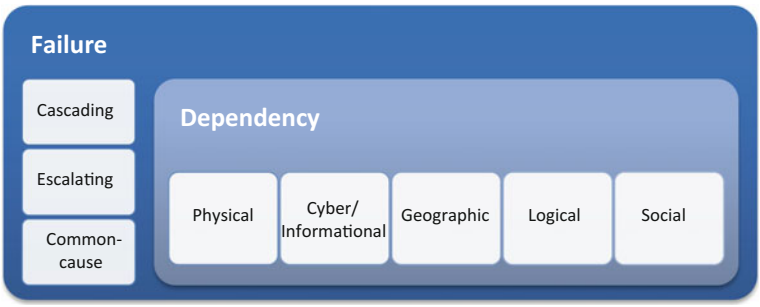

Fig. 2 Taxonomy of dependency and failure adapted by [1, 8]

these data. Since most of these approaches are historically based they can be used in order to predict similar, known failures, but they do not provide good prediction capability for unknown or new incidents. These weaknesses call for other simulation approaches for additional decision support, which we will also examine later in this chapter (Fig. 2).

On the base of the approaches used to investigate the dependency phenomena we can identify three main categories of modeling: Holistic, Topologic and Simulation-based.

Holistic approaches These approaches adopt more simplified models able to provide, with some approximation, qualitative information about the phenomena. Generally, they assume that each infrastructure can be modeled as a single entity, which depends for its correct behavior or performance on the availability of services provided by other infrastructures (other entities).

They generally adopt economic or empirical data as source of information to infer dependencies, such as history data of failures, incidents or disruptions, as well as experts opinions. A typical example of such approaches is the economic and 'inoperability' metrics used for dependency modeling [16]. Ouyang [17] argues that such empirical studies are used in order to: "identify frequent and significant failure patterns, quantify interdependency strength metrics to inform decision making, make empirically-based risk analysis, and provide alternatives to minimize the risk".

Holistic approaches generally operate with macro-scale aggregated information that can be acquired with relatively reduced effort [18]. This largely facilitates the set-up of the models. They are usually the starting point of such analysis and they can be used when sensitive data cannot be exchanged among stakeholder because of the possibility of agreeing an acceptable level of abstractions. At the same time, it may be introduced a bias to the results, over- or under-estimating some aspects with respect to others. The information obtained by such methodologies is not suitable for operative analysis.

Network-based approaches These approaches assume that each infrastructure is composed by a set of identical elements (generally represented as a node on a

graph), while dependencies are inferred assuming some sort of relationship existing among nodes belonging to different networks [19, 20, 21]. **Topology-based or structural** approaches generally identify discrete states for each component (node or link) and usually with two states: failed and normal, i.e., each node is either fully working or completely out-of-work. To implement these approaches in their basic formulation it is enough to have the topological structure of the infrastructure (which is a quite easy data to obtain). This static formulation is able to capture the 'structural' properties of the network. These approaches usually examine failures at the node or link level, and then examine cascading failures to other nodes or links within the network. They are used to evaluate the robustness of a network from the topological perspective, e.g. using centrality measures [22]. Further useful methods are illustrated in Chap. 6.

However, in several cases, e.g., for a telecommunication network, topologic analyses are unsatisfactory because the static properties of the network do not have immediate consequences on its capability to provide the intended services. To overcome such limit, some authors as Rosato et al. [23] suggested to consider also network dynamics and, to this end, they equipped the topological structure with some kind of flow dynamic models (**flow-based** models) (see also [17]). Flow-based methods depict the level of services exchanged between nodes or the flow in the graph. In this case, each node can deliver to, or consume a service from another node. Such approaches offer a depiction, which is closer to reality, and they are also used to identify critical nodes or links in the graph. The problem is that the data required to tune such dynamic models is hard to obtain and the computational cost is very high as the network grows. In most cases, and depending on the level of detail, such network-based approaches are analyzed further by simulation methods.

Simulation-based approaches These approaches try to discover the dependency phenomena as emerging from the behavior of single components and parts. Hence, they are generally able to consider a continuous level of degradation in the component functionalities and the concurrent presence of several types of phenomena (like absence of resources, external failures and internal dynamics). Starting from the component-based behavior, they try to obtain information about the 'dependence' existing among the infrastructures. Generally, these approaches are intrinsically quantitative and operation oriented. Substantially these methodologies use simulation framework to estimate the impact induced by a given failure to a scenario composed by several heterogeneous infrastructures (see [24–27]). Unfortunately, for the phenomena under analysis, a more detailed model does not necessarily mean a more accurate model. Indeed, the complexity of such simulation platforms mask, in several cases, a large number of subjective hypotheses, which influences the correctness of the solutions.

As illustrated in Fig. 3, holistic approaches are more easy to develop and set-up due their level of abstraction, but they are fundamentally strategy-oriented. On the other side, simulation-based solutions are able to give operative information, but they require more computational overhead and more detailed models. The latter represents a serious drawback because, in the field of critical infrastructure, it is

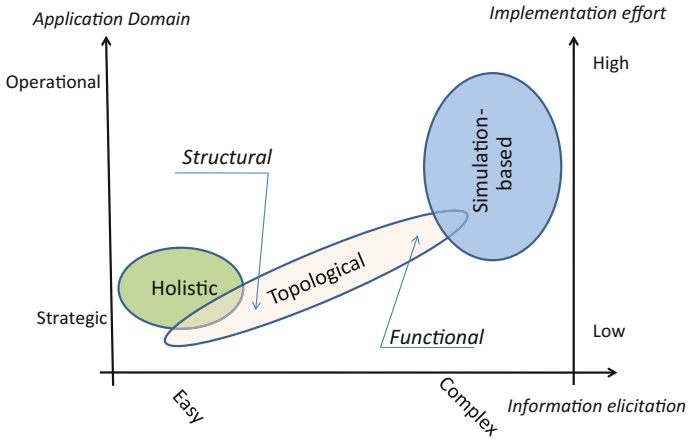

Fig. 3 Taxonomy of dependency modeling approaches [7]

very difficult to collect such detailed data due to the reluctance of the operators to provide such sensitive data, and also because of the huge quantity of highly time-varying data that should be collected. In the middle, we have the networked based approaches, which, for some aspects, share some of the advantages and weaknesses of both previous classes. Indeed, their most simple formulation (that referred as 'structural') is quite easy to set-up, since only the topological structure of the involved systems is required. Conversely, when there is the need to consider also the 'functional' properties of the network, the complexity of the model grows fast and it becomes comparable with simulation-based approaches. The topological approach, in a scenario composed of two infrastructures, where there is a single predominant (e.g., physical) dependency mechanism, is able to provide more 'objective' measurements rather than holistic models of comparable effort. Unfortunately, the extension to more complex scenarios is not straightforward and requires to collected huge quantity of resources.

In the rest of the chapter we illustrate in more detail the first two classes (which will be further analyzed in Chap. 6), while the other chapters of the book are dedicated to illustrate the different elements and aspects related with the simulation based approach.

In [17] the authors have catalogued about 150 approaches using a six classes taxonomy where the methods are not split on the level of granularity of the data but on the type of information used in the six classes:

- *Empirical approaches*: The analysis of the dependencies is performed on the base of historical accidents or disaster data and past expert experiences. These methods allow to identify frequent and significant failure patterns, to quantify (inter)dependency indicators and perform empirically-based risk analyses;
- *Agent based approaches*: These approaches follow a bottom-up method assuming that the complex behavior emerges from many individual and

relatively simple interactions of autonomous agents (i.e. adopting a complex adaptive systems (CAS) methodology).
- *System dynamics approaches*: which use System Dynamic framework to analyze complex systems involving interdependencies on the base of top-down method.
- *Economic theory based approaches*: where dependencies are identified on the base of economic exchanges among sectors and infrastructures on the base of Input–output methods.
- *Network based approaches*: Infrastructure are described by networks, where nodes represent different components and show the existing (physical) relationship among them. Such class includes topology-based and flow-based methods.
- Other approaches: which collect other methods based on hierarchical holographic modeling (HHM), high level architecture (HLA), petri-net (PN), dynamic control system theory (DCST), Bayesian network (BN), etc. For more details see [17] and the reference therein.

Other classifications of approaches are also available in the literature [52–54].

5 Holistic Approaches

Holistic approaches are based on the concept of 'service degradation', in order to illustrate how degradation within one infrastructure (or sector or component) is able to influence the capability to operate of other infrastructures.

These approaches are generally abstract, simplified and strategic oriented. They can be set-up quite easily, as they do not require as detailed data as other approaches. Even if several important aspects are neglected (e.g., the geographical dispersion that characterizes several infrastructures), they are "compact and understandable"; moreover, they can consider, at the same time, several infrastructures and dependency mechanisms (even if they all reduce to a single abstract parameter, e.g., inoperability). Finally, these approaches are service oriented.

IIM In this framework, the most popular approach is the input-output inoperability model (IIM), introduced in [16] as an evolution of the economic theories of the Nobel Prize Leontief [28]. IIM uses the same theoretical framework proposed by Leontief, but instead of considering how production of goods of a firm influences the level of production of the other firms, it focuses on the spread of operability degradation among the networked system. The most significant idea introduced in this paper was the concept of 'inoperability', intended as the inability of an element to perform its prescribed functions. This concept can be assumed as one of the 'lowest common denominator' allowing to measure with a single abstract parameter several types of relationships. For the same intent in Macaulay [18], the author suggests to use a monetary equivalent.

With a high level of approximation, the approach assumes that each infrastructure is modeled as a single entity, whose level of operability depends on the

availability of "resources" supplied by the other infrastructures. Then, an event (e.g., a failure) that reduces the operational capability of the i-th infrastructure may induce degradation also in the other infrastructures, which require goods or services produced by the i-th one. These degradations may be further propagated to other infrastructures (cascading effect) and even exacerbate the situation of the i-th one due to the presence of feedback loops.

Mathematically, IIM describes these phenomena on the basis of the level of inoperability associated to each infrastructure. Following the economic equilibrium theory of Leontief [28] a static demand-reduction model [16, 29] for n infrastructures is given by:

$$\Delta x = A^* \Delta x + \delta c^*$$

where Δx is the difference between the planned production (x_0) and the degraded production (x_d) production, δc^* is the difference between the planned final demand (c_0) and the degraded final demand (c_d), and A* is a square n × n matrix whose elements a_{ij} (Leontief technical coefficients) represent the ratio of the input from the i-th infrastructure to the j-th one with respect to the overall production requirements for the j-th infrastructure. Starting from [30] and introducing the following transformation [29]:

$$x = [diag\{x_0\}]^{-1} \Delta x = P \Delta x$$

We obtain the static input-output inoperability relation

$$\boldsymbol{x} = PA^*P^{-1}\boldsymbol{x} + Pc^* = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c} \tag{1}$$

where $\boldsymbol{x}$ and $\boldsymbol{c}$ are the vectors composed, respectively, by the level of inoperability and by the external failure and $\boldsymbol{A}$ is the influence matrix, i.e. the matrix elements a_{ij} of such matrix represent the fraction of inoperability transmitted by j-th infrastructure to i-th one or, in other terms, how much the inoperability of j-th infrastructure influences i-th infrastructure.

The overall inoperability corresponding to a perturbation c is given by:

$$\boldsymbol{x} = (I - A)^{-1}\boldsymbol{c} = \boldsymbol{S}\boldsymbol{c} \tag{2}$$

In the following, let us refer to A and $S = (I - A)^{-1}$ as the open-loop and closed-loop dependency matrices, respectively. Matrix A models the direct effects due to first-order dependencies while matrix S also takes into account the amplifications introduced by domino effects (i.e., second-order and higher-order dependencies). Notice that, under suitable hypothesis of matrix A, of the closed loop dependency matric S can be expressed as

$$S = (\boldsymbol{I} - \boldsymbol{A})^{-1} = \boldsymbol{I} + \boldsymbol{A} + \boldsymbol{A}^2 + \boldsymbol{A}^3 + \cdots$$

Such an equation provides an immediate understanding of the cumulative effects of high-order dependencies in matrix S. i.e. the sum of the direct (first), second, third and so on order of interdependencies.

To quantify the role played by each infrastructure, in [31] the authors introduced the dependency index, defined as the sum of the Leontief coefficients along the single row

$$\delta_i = \sum a_{ij} \tag{3}$$

and the influence gain, i.e., the column sum of the Leontief coefficients

$$\rho_j = \sum a_{ij} \tag{4}$$

Where the first index measures the robustness of the infrastructure with respect to the inoperability of other infrastructures. As a matter of fact, it represents the maximum inoperability of the i-th infrastructure when every other infrastructure is fully inoperable. The lower the value, the greater the ability of the i-th infrastructure to preserve some working capabilities (e.g., using buffers, back-up power, etc.) despite the inoperability of its supplier infrastructures.

On the other side influence gain conversely, measures the influence exerted by one infrastructure over the others. A large influence gain means that the inoperability of the j-th infrastructure induces significant degradations to the entire system.

However, as illustrated in [32] such indices refer only to the direct influence exerted or suffered by each infrastructure. In other terms, those indices do not consider the consequences of second or higher order interdependencies, i.e. the effects induced by multi-step cascading phenomena. These overall effects can be evaluated considering the closed-loop matrix S.

As an example for the IIM, Fig. 4 (left) reports a simplified scenario, which include three infrastructures with the relative influence coefficient and, on the right, the corresponding IIM model.

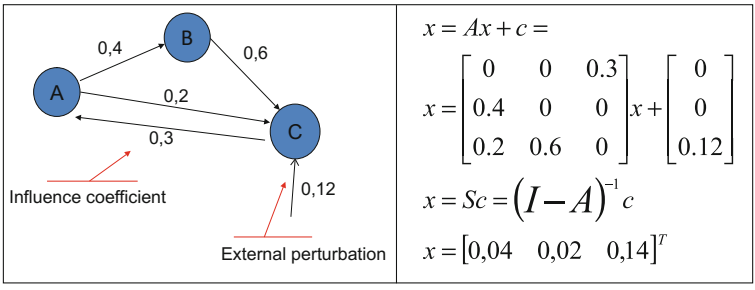

Fig. 4 Example of IIM model for 3 dependent infrastructures

The analysis of the matrix A allows to discover that infrastructure C is the most dependent one with a dependency index of 0.8, while infrastructure A and B are those with the highest influence index $\rho_A = \rho_B = 0.6$.

Equation [2] can be used to estimate, for example, the overall effect of an external perturbation able to reduce the inoperability of infrastructure C of the 12% (i.e. $c = [0 \quad 0 \quad 0.12]^T$). The result $x = [0.04 \quad 0.02 \quad 0.14]^T$ shows that infrastructure A suffers an operability reduction of the 4%, the double of those suffered by infrastructure B, but also that the inter-dependency phenomena exacerbate the negative consequences on the infrastructure C which inoperability level grows up to the 14%.

The static input–output inoperability model defined in Eq. [30] can be extended in the Dynamic IIM (DIIM) by incorporating a dynamic term:

$$\dot{\boldsymbol{x}}(t) = K(A - I)\boldsymbol{x}(\boldsymbol{t}) + K\boldsymbol{c} \tag{5}$$

where $\dot{x}(t)$ represents the variation in the inoperability level at time t and the diagonal matrix normal economic conditions is referred to the industry resilience coefficient matrix because each element k_{ii} measures the resilience of the i-th infrastructure in terms of recovery rate with respect to adverse or malicious events.

The DIIM can be used to analyze the evolution of the inoperability in an inter-dependent scenario until an equilibrium, if any, is reached,[1] as illustrated in Fig. 5 for the example of Fig. 4.

In many application scenarios, however, it is more useful to consider a discrete-time representation of [5]. Given a sampling rate Ts, a discrete time model can be obtained approximating the derivative with the incremental ratio.

$$\boldsymbol{x}(k) = A\boldsymbol{x}(\boldsymbol{k}) + \boldsymbol{c} + \boldsymbol{B}[\boldsymbol{x}(\boldsymbol{k}+1) - \boldsymbol{x}(\boldsymbol{k})] \tag{6}$$

In the case the restoration phase is neglected, i.e. $B = -I$ Eq. [24] simplify in

$$\boldsymbol{x}(k) = A\boldsymbol{x}(\boldsymbol{k}) + \boldsymbol{c}$$

Often for the discrete-time interdependency model one can directly assess the values of the elements of matrix A for example via interview with sectors' experts [33, 32].

The paper of Haimes and colleagues had a large influence and inspired several extensions and particularizations of IIM, which were applied in different contexts to estimate the impact of catastrophic events and major terrorist attacks [29, 34, 35]. However, one needs to note that such models cannot model dependencies at the

[1] An equilibrium condition exists only if the system is stable, i.e. if all the eigenvalues of (I-A) have a strictly negative real part. Notice that the stability of the system does not dependent on the particular matrix K.

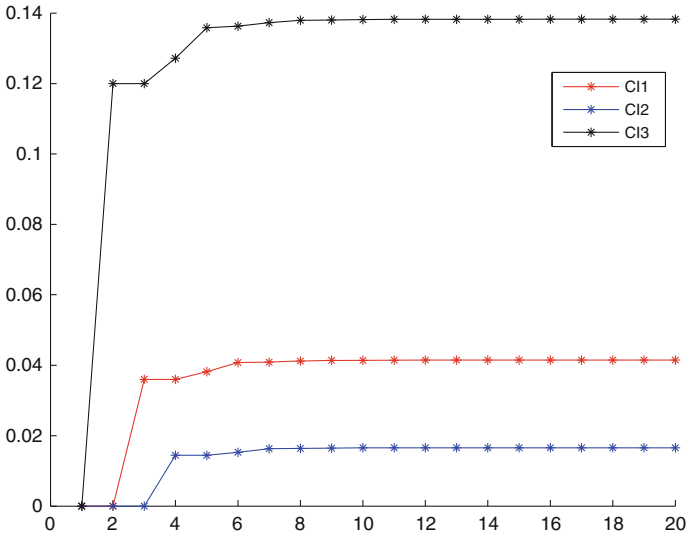

Fig. 5 Evolution of discrete time DIIM for system of Fig. 4

component level, but offer a more macroscopic view. Also, the dependencies identified are derived by normal economic conditions [17].

Similar results can be obtained using System Dynamics (SD) approach. SD is a methodology and a computer simulation modeling technique for framing, understanding, and discussing the dynamic behavior and no-intuitive casual relationships among variables in complex systems. Originally introduced by Jay W. Forrester in the 1960s and used to help corporate managers to improve their understanding of industrial processes [36], SD has been also used in the framework of CI to overcome limits related to the use of past data to predict the future. Indeed, the SD aim to identify individual causalities and how they combine to create feedback loops that are the causes of the counter-intuitive outcomes. It is important to point out that the expected outcomes are not quantitative predictions for a particular variable, but rather a measure of the dynamic behavior pattern of the system, given the inputs and the conditions in the model.

The core of the SD strategy consists in representing the system structure in terms of stocks, flows, and the causal mechanisms that govern their rates of change. Stocks represent quantities or states of the system, the levels of which are governed over time by flow rates between stocks. In SD the dependencies among CI are modelled via two diagrams: causal-loop diagram capturing the causal influence among different variables and stock-and-flow diagram describing the flow of information and products through the system.

Figure 6, for example, presents a causal loop diagram aimed to capture the possible effects of the implementation of policies designed to reduce terrorist acts [37].

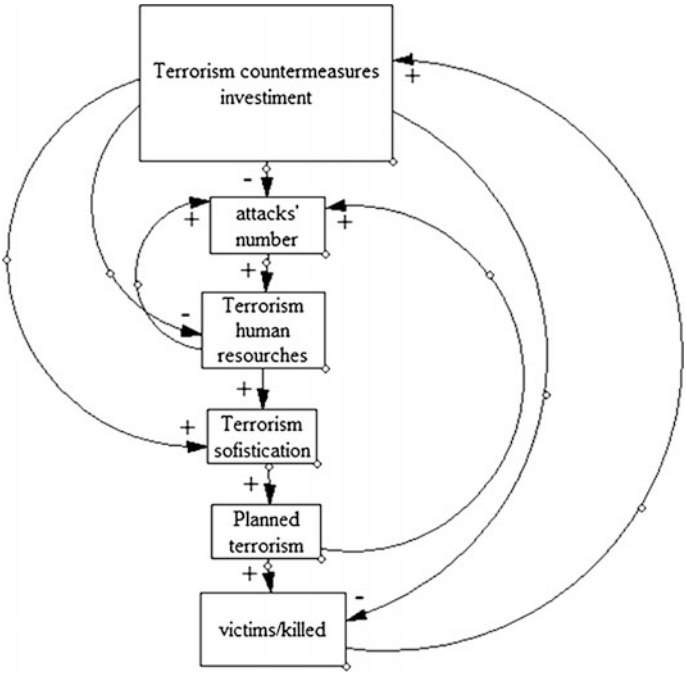

Fig. 6 Example of causal loop diagram of a system dynamic model (modified from [37])

The arrows that link each variable indicate places where a cause and effect relationship exists while the plus or minus sign at the head of each arrow indicates the direction of causality between the variables, when all the other variables (conceptually) remain constant.

The causal diagram shown in Fig. 6 can be interpreted in the following way. As the Government increases its investment in anti-terrorism countermeasures, the number of the perpetrated attacks and the number of terrorist human resources decrease. On the other hand, the anti-government sentiment (as felt by extremist groups) increases. This sparks the hatred extremist groups that use religion, force and/or political causes to obtain resources and recruit more members. Therefore, terrorist human resources (recruitment) increase. As terrorist human resources increase, also terrorist sophistications (strength, lethality and/or capability) increase. And as a consequence, the number of terrorist attacks (planned or not) increases as well. These give a boost to the number of victims, causing the increment, by the Government, of the terrorism-defense resource allocation.

Substantially, SD models the dynamic and the evolutionary behavior of CI scenario trying to capture the most relevant causes and effects relationships under disruptive scenarios. SD allows to include in the model the effects of investments and policy and technique factors to reflect the system evolution in the long term.

SD has been used to perform risk analysis in complex scenarios [38, 39, 33] to analyze the criticality in railway station [40], to improve crisis management in the presence of extreme events [41], so as to design sophisticated tools as CIP/DSS [42].

The main weaknesses of SD is that the causal loop diagram is established based on the knowledge of a subject matter experts. Moreover, being a semi-quantitative method, it use a series of differential equations to describe the system-level behaviors of the CI and this requires the calibration of many parameters and functions in the models, which need a huge amount of data [17].

6 Networked Based Approaches

These approaches try to infer information on dependencies representing the different elements as "nodes" of a network where the presence of a relation between two nodes is depicted via a link connecting them. Their most interesting features are the relative simplicity and the inductivity of the relative assumptions, especially when referred to physical interdependencies. Indeed, the most natural approach is to represent the different components of an infrastructure as the nodes of the network where the links represent their relationship/connection.

Exploiting the powerful toolset provided by graph theory it is possible to characterize the relevance of the different nodes, so as the properties of the whole network [30]. This type of analysis can emphasize that several technological networks due to their peculiar topological structure (generally referred as "scale-free" [43]) are very robust with respect to accidental failure, but at the same time they are very fragile to deliberate attack.

Recently several authors suggested using this approach to analyze also dependency between different CI. In this type of approaches, the physical couplings are mainly considered assuming that the primary source of interdependency is geographical proximity. Here the concept of geographical proximity (that stresses the influence of two nodes in close spatial proximity) embraces, generally, physical and geographical dependencies, as defined by Rinaldi et al. [1].

The underlying idea of these approaches is illustrated in Fig. 7. The figure demonstrates how a perturbation occurred into one graph representing a network is able to influence the properties of another graph representing a second infrastructure (network).

In order to apply such an approach, the researchers have to preliminarily assume:

- *The topological (and eventually dynamic) model of the first infrastructure*, i.e. the nodes and the arcs of the network (and for the dynamic model the flow model to adopt);
- *The topological (and eventually dynamic) model of the second infrastructure*, i.e. the nodes and the arcs of the network (and for the dynamic model the flow model to adopt);

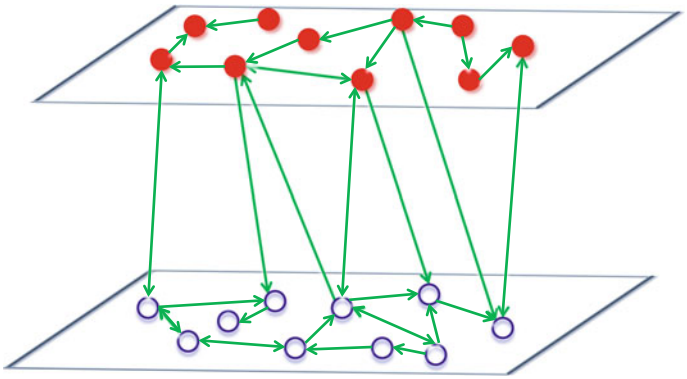

Fig. 7 Topological approaches are based on network-oriented modeling

- *The coupling mechanism existing among the nodes of the two networks*, i.e. how the nodes of the first infrastructure are linked to the ones' of the second infrastructure and vice versa (and for the dynamic model also a threshold mechanism).

Today, the structural vulnerability is one of the most applied tools (see for example [20, 44–48] and the references therein). It is not clear if this is due to the intrinsic importance of such types of relations, or because it is the only approach for which it is feasible to acquire the needed data. However, some authors emphasize that the analysis of structural properties is not able to provide always coherent and exhaustive data.

To overcome such limits, different authors started to consider also the "functional" properties of the network. To this end it is assumed that some form of fluxes "flows" over the networks and it is investigated how a topological event occurred in a network (e.g. the removal of a node or a link) influences the fluxes existing in the other network.

Even if in the literature there are several studies devoted to the functional analysis of a single infrastructure, only recently some studies about coupled infrastructures appeared [19, 49].

The results reported in the literature emphasize how structural and functional vulnerabilities are substantially poorly correlated concepts that capture different properties, i.e. two networks should be strongly coupled from the structural point of view, and at the same time lightly coupled when considering the functional properties and vice versa. Unfortunately, there are no final indications about which one of these properties is the most relevant neither to explain those apparently incoherencies. However, to perform a functional vulnerability assessment, not only is it mandatory to acquire information about the topological structure of the network, but also a model about the characteristics of the fluxes and their specific parameters. This introduces several degrees of freedom into the model that may lead to erroneous conclusions.

In [20] the authors consider the coupling of networks able to reproduce the real structure of a small-scale water and gas networks. They introduce a simple rule to establish interdependencies among networked elements based upon geographical proximity. The work is devoted to investigate, with reference to a set of topological parameters (vertex degree, clustering, characteristic path length, redundancy ratio) the effects of coupling. To this end they introduced a tunable parameter that drives the networks from isolation to complete interdependency.

In [50] it is addressed the problem of interdependent response dividing the problem into analysis of static topological properties, and analysis of the effects of those properties in dynamic response. Dynamic response is investigated through time-dependent properties such as network resilience and fragmentation modes. Using a small-world network model, variation of topological properties as a function of disruption severity is analyzed. Efforts are made to determine if correlations exist among failure models, network component removal strategies, and network topology.

In [21] there is an attempt to formalize the interdependent dynamics among several heterogeneous infrastructures. In this framework a metric for the level of functionality of an infrastructure is given by the sum of the functionality of the infrastructure components divided by the number of components. This approach has been used in [21] to analyze the interconnection of electric grid and telephony network: to investigate the effect, on the telephony network, of removing from the power distribution network one or two nodes, they introduce as metric the remaining fraction of functional telecommunication nodes.

A similar formalism has been proposed in [51] where five types of infrastructure are presented and incorporated into a network flow framework and tested with reference to the lower Manhattan region of New York.

In the framework of functional analysis, an interesting result is proposed in [23] where the interconnection properties of an electric grid and a TLC network that mimic the Italian situation are investigated. The authors used the DC power flow to model the electric flux and developed a specific model to address the packet routing in the TLC network. In this paper the effect of the interdependency is measured in terms of degradation of the QoS (Quality of Service). Specifically, the metric adopted for the electric QoS is the fraction of dispatched power with respect to the nominal load and for TLC the increment in the dispatching time with respect to the unperturbed situation. Then they evaluate how the degradation experimented in the electric QoS affects the TLC QoS.

7 Conclusions

To summarize, all approaches mentioned and analyzed, rely heavily on the availability of high quality data in order to ensure a realistic representation of the CI topology, behavior and failure consequences. In general, this type of data is difficult to obtain and handle either due to their sensitivity or to their volume. Moreover,

there is no standardized data collection methodology for interdependent CI and thus the wider application of such models is hindered.

Even if this data is collected for a first analysis, repeating such an exercise and keeping the data up to date requires significant resources and investments by the industry. Even if in the very last years there is more attention and availability from stakeholder to share data, focusing on approaches that can be easily updated is a significant requirement.

The validation of this type of models is an important step, which is usually neglected, partially due to the lack of real data to test these approaches. Moreover, current models often incorporate theoretical assumptions or abstractions, poses significant challenges when practically applied.

Finally, we observed that the various available methods cover different aspects of the problem and there is the need to combine them in order to battle some of their shortcomings. Integrating or federating models allowing them to exchange data is not a trivial task and we will investigate it further in the following chapters.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author (s).

References

1. Rinaldi SM, Peerenboom JP, Kelly TK (2001) Critical infrastructure interdependencies. IEEE Control Syst Mag, 11–25
2. Andersson G, Donalek P, Farmer R, Hatziargyriou N, Kamwa I, Kundur P, Martins N, Paserba J, Pourbeik P, Sanchez-Gasca J, Schulz R, Stankovic A, Taylor C, Vittal V (2005) Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance. IEEE Trans Power Syst 20(4):1922–1928
3. Hokstad P, Utne IB, Vatn J (2012) Risk and interdependencies in critical infrastructures. Springer series in reliability engineering. Springer, London
4. Klaver MHA, Luiijf HAM, Nieuwenhuijs AN, van Os N, Oskam V (2016) Critical infrastructure assessment by emergency management. In: CLecture Notes in Computer Science, vol 9568, Springer, Heidelberg, 2016, pp 79–90
5. Barrett C, Beckman R, Channakeshava K, Huang F, Kumar V, Marathe A, Marathe M, Pei G (2010) Cascading failures in multiple infrastructures: from transportation to communication network. In: 5th international conference on critical infrastructure (CRIS), pp 1–8
6. Nieuwenhuijs A, Luiijf E, Klaver M (2008) Modeling dependencies in critical infrastructures. In: Goetz E, Shenoi S (eds) Critical infrastructure protection, IFIP Series, vol 253, pp 205–214
7. Setola R (2010) How to measure the degree of interdependencies among critical infrastructures. Int J Syst Syst Eng 2(1):38–59
8. De Porcellinis S, Panzieri S, Setola R (2009) Modelling critical infrastructure via a mixed holistic reductionistic approach. Int J Crit Infrastruct 5(1–2):86–99

9. Dudenhoeffer DD, Permann MR, Manic M (2006) CIMS: a framework for infrastructure interdependency modeling and analysis. In: Proceedings of the 38th conference on Winter simulation, Dec 2006, pp 478–485
10. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA, van Eeten MJG, Cruz E (2010) Empirical findings on European critical infrastructure dependencies. Int J Syst Syst Eng 2(1):3–18
11. Van Eeten M, Nieuwenhuijs A, Luiijf E, Klaver M, Cruz E (2011) The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Adm 89(2):381–400
12. Bologna S, Macdonald R (2002) Advanced modeling and simulation methods and tools for critical infrastructure protection. ACIP Project
13. U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: causes and recommendations (2004)
14. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA (2008) Critical infrastructure dependencies 1-0-1. In: First international conference on infrastructure systems and services: building networks for a brighter future (INFRA), 2008, Rotterdam, pp 1–3
15. Aung Z, Watanabe K (2009) A framework for modeling interdependencies in Japan's critical infrastructures. In: Palmer C, Shenoi S (eds) 3rd IFIP international conference on critical infrastructure protection (CIP-2009). Springer, USA, pp 243–257
16. Haimes YY, Jiang P (2001) Leontief-based model of risk in complex interconnected infrastructures. J Infrastruct Syst 1–12
17. Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 121:43–60. ISSN 0951-8320
18. Macaulay T (2008) Critical infrastructure. CRC Press, Boca Raton
19. Carreras BA, Newman DE, Gradney P, Lynch VE, Dobson I (2007) Interdependent risk in interacting infrastructure systems. In: Proceedings of the 40th Hawaii international conference on system sciences, 2007
20. Duenas-Osorio L, Craig JI, Goodno BJ, Bostrom A (2007) Interdependent response of networked systems. J Infrastruct Syst 185–194
21. Svendsen NK, Wolthusen SD (2007) Analysis and statistical properties of critical infrastructure interdependency multiflow models. In: Proceedings of IEEE workshop on information assurance, pp 247–254
22. Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Gritzalis D (2015) Risk mitigation strategies for critical infrastructures based on graph centrality analysis. Int J Crit Infrastruct Prot 10:34–44
23. Rosato V, Issacharoff L, Meloni S, Tiriticco F, De Porcellinis S, Setola R (2008) Modelling interdependent infrastructures using interacting dynamical models. Int J Crit Infrastruct (IJCIS) 4(1/2):63–79
24. Bologna S, Casalicchio E, Masucci V, Setola R (2008) An integrated approach for simulating interdependencies. In: Papa M, Shenoi S (eds) Critical infrastructure protection II. Springer, Boston, pp 221–231
25. De Porcellinis S, Panzieri S, Setola R, Ulivi G (2008) Simulation of heterogeneous and interdependent critical infrastructures. Int J Crit Infrastruct (IJCIS) 4(1/2):110–128
26. EU project DIESIS (Design of an Interoperable European federated Simulation network for critical Infrastructures), Deliverable "D2.3 Report on available infrastructure simulators" http://www.diesis-project.eu/
27. Pederson P, Dudenhoeffer D, Hartley S, Permann M (2006) Critical infrastructure interdependency modelling: a survey of U.S. and international research. Idaho National Lab, 2006
28. Leontief WW (1951) The structure of the American Economy 1919–1939. Oxford University Press, Oxford
29. Haimes Y, Horowitz B, Lambert J, Santos J, Lian C, Crowther K (2005) Inoperability input–output model for interdependent infrastructure sectors. I: theory and methodology. J Infrastruct Syst 11(2):67–79

30. Albert R, Barabasi A (2002) Statistical mechanics of complex networks. Rev Mod Phys 74:48–97
31. Setola R, De Porcellinis S (2008) A methodology to estimate input-output inoperability model parameters. In: Critical information infrastructures security 2007. Lecture Notes in Computer Science. Springer, Berlin, pp 149–160
32. Setola R, De Porcellinis S, Sforna M (2009) Critical infrastructure dependency assessment using input-output inoperability model. Int J Crit Infrastruct Prot (IJCIP) 170–178
33. Laugé A, Hernantes J, Sarriegi JM (2015) Critical infrastructure dependencies: a holistic, dynamic and quantitative approach. Int J Crit Infrastruct Prot 8:16–23
34. Santos JR (2006) Inoperability input-output modeling of disruptions to interdependent economic systems. J Syst Eng 20–34
35. Santos JR (2008) Inoperability input-output model (IIM) with multiple probabilistic sector inputs. J Ind Manag Optim 489–510
36. Forrester JW (1961) Industrial dynamics. MIT Press, Cambridge, MA
37. Madnick S, Siegel M (2008) A system dynamics (SD) approach to modeling and understanding terrorist networks. Massachusetts Institute of Technology, Cambridge
38. Brown T, Beyeler W, Barton D (2004) Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems. Int J Crit Infrastruct 1(1):108–117
39. Cavallini S, d'Alessandro C, Volpe M, Armenia S, Carlini C, Brein E, Assogna P (2014) A system dynamics framework for modeling critical infrastructure resilience. In: International conference on critical infrastructure protection, Mar 2014. Springer, Berlin, pp 141–154
40. De Cillis F, De Maggio MC, Setola R (2015) Vulnerability assessment in RIS scenario through a synergic use of the CPTED methodology and the system dynamics approach. In: Railway infrastructure security. Springer International Publishing, pp 65–89
41. Santella N, Steinberg LJ, Parks K (2009) Decision making for extreme events: modeling critical infrastructure interdependencies to aid mitigation and response planning. Rev Policy Res 26(4):409–422
42. Bush B, Dauelsberg L, LeClaire R, Powell D, DeLand S, Samsa M (2005) Critical infrastructure protection decision support system (CIP/DSS) overview. Los Alamos National Laboratory Report LA-UR-05-1870, Los Alamos, NM 87544
43. Albert R, Jeong H, Barabasi A (2000) Error and attack tolerance of complex networks. Nature 406:378–382
44. Bompard E, Napoli R, Xue F (2009) Analysis of structural vulnerabilities in power transmission grids. Int J Crit Infrastruct Prot 2(1):5–12
45. Chopra SS, Dillon T, Bilec MM, Khanna V (2016) A network-based framework for assessing infrastructure resilience: a case study of the London metro system. J R Soc Interface 13 (118):20160113
46. Latora V, Marchiori M (2005) Vulnerability and protection of infrastructure networks. Phys Rev E 71(1):015103
47. Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ (2011) Mitigation of malicious attacks on networks. Proc Natl Acad Sci 108(10):3838–3841
48. Zhang Y, Yang N, Lall U (2016) Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. J Syst Sci Syst Eng 25(1):102–118
49. Kurant M, Thiran P (2006) Layered complex networks. Phys Rev Lett 96:138701
50. Duenas-Osorio L, Craig JI, Goodno BJ (2008) Probabilistic response of interdependent infrastructure networks
51. Lee EE, Mitchell JE, Wallace WA (2007) Restoration of services in interdependent infrastructure systems: a network flow approach. IEEE Trans Syst Man Cybern Part C 37 (6):1303–1317
52. Kröger W, Zio E (2011) Vulnerable systems. Springer, London. ISBN 978-0-85729-654-2
53. Rinaldi S (2004) Modeling and simulating critical infrastructures and their interdependencies. In: 37th Hawaii international conference on system sciences, vol 2, USA. IEEE

54. Zio E, Sansavini G (2011) Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Trans Reliab 60(1):94–101

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.