# Modeling and simulation of critical infrastructures

Gabriele Oliva[1], Stefano Panzieri[1] & Roberto Setola[2]
[1]*University Roma Tre of Rome, Italy*
[2]*University Campus Bio-Medico of Rome, Italy*

## Abstract

While the knowledge of human operators and stakeholders is becoming more and more sector specific, infrastructures are becoming more and more interoperable and interdependent. Hence representing the behavior and the characteristics of such a scenario is a mandatory task, in order to assess the risk of multiple disruptions and domino effects, and in order to provide adequate policies and countermeasures to react to structural vulnerabilities, failures, or even intentional attacks. In the literature many approaches have been proposed; *holistic* methods consider infrastructures with an high level of abstraction, while *topological* frameworks consider the interaction of multiple homogeneous subsystems. Nevertheless, *simulative* approaches are focused on a detailed representation of isolated subsystems or *agents*, evaluating their interaction by means of simulation platforms. Finally multilayer methodologies consider interconnected agents according to multiple levels of abstraction or perspectives.

*Keywords*: Critical Infrastructures, Interdependency Modeling, System of Systems

## 1 Introduction

The representation of *interdependency* is a fundamental task for the comprehension of the relations that exist between infrastructures and subsystems, in order to quantify threats, identify structural vulnerabilities, and define adequate countermeasures, policies, and strategies. This is the goal of the so-called *Critical Infrastructure Protection* (CIP) strategies developed by several governments and international organizations [1].

Indeed infrastructures are becoming so relevant to be *critical* for the welfare, economy, and security of any developed countries; in fact any disruption or failure in these complex systems "would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning

WIT Transactions on State of the Art in Science and Engineering, Vol 54, © 2012 WIT Press
www.witpress.com, ISSN 1755-8336 (on-line)
doi:10.2495/978-1-84564-562-5/03

of governments" [2]. However, while modeling and simulation techniques are well-established for the single infrastructure, the representation of highly coupled and interdependent infrastructures is still immature.

In recent years infrastructures have reached an high degree of interoperability, mainly due to the pervasiveness of Information and Communications Technologies (ICT) in fact cyber inter-dependency potentially couples an infrastructure with every other one, in spite of their nature, type, or geographical location [3]. Moreover, because of the huge growth of the complexity of each infrastructure, the skills of technicians, operators, and stakeholders are becoming more and more sector specific. Therefore, while it is often possible to retrieve exhaustive information about the behavior of any single infrastructure and its elements, cross-infrastructure inter-dependencies are often implicit, hidden or neither well understood by the same stakeholders.

In this chapter the state of the art in the representation, analysis, and simulation of interdependent critical infrastructures is reviewed. The chapter is organized as follows: After a preliminary overview of interdependency modeling and simulation (Section 2), *Holistic* modeling approaches are described in Section 3; Section 4 reviews *topological analysis*, both from the structural (Section 4.1) and functional (Section 4.2) points of view; *simulative* frameworks are depicted in Section 5, further describing *Agent-Based* (Section 5.1) and *Multilayer* (Section 5.2) methodologies; finally some conclusive remarks are collected in Section 6.

## 2 Interdependency modeling

In order to review the state of the art of interdependency modeling and simulation techniques, there is the need to provide some initial definitions.

The *inoperability* of an infrastructure or subsystem is the inability to perform its intended function. A *failure* is a negative event that influences the inoperability of infrastructures and subsystems; a failure can also be propagated or propagate its effects, according to specific concepts of proximity. An infrastructure or subsystem $A$ is *dependent* on another infrastructure or subsystem $B$ when a degradation of $B$, that is, an increment of its level of inoperability, induces a degradation into $A$ [4]. Obviously, $A$ and $B$ are *interdependent* if they are mutually dependent.

These definitions are very general and, besides including evident and direct dependencies, embrace more complex behaviors, such as amplifications, domino effects, and loops.

Indeed, in highly interdependent scenarios, a degradation in one infrastructure or subsystem may generate consequences on the others, which are not easy to represent. For instance, a failure in a given infrastructure may induce degradations into another one; this may induce some further degradation into the first infrastructure, exacerbating the original problem, and so on. Another relevant example is *indirect* (inter)dependency; in this case two infrastructures or subsystems may be (inter)dependent even if they do not directly interact, that is, when their interaction is mediated by means of a chain of (inter)dependencies.

In the literature many approaches have been proposed to address the problem of interdependent critical infrastructures; these methods are, typically, adopted in order to perform "what if?" analyzes and ex-post simulations, with the aim to understand structural vulnerabilities, to asses and mitigate the risk of domino effects and multiple disruptions, and to provide a support to decision makers. In [3], the authors emphasize how dependency and interdependency should be analyzed with respect to different dimensions. In particular they catalog dependencies into four, not mutually exclusive, classes:

- *Physical dependency*: Two infrastructures are physically dependent if the operations of one infrastructure depend on the physical output of the other.
- *Cyber dependency*: An infrastructure presents a cyber dependency if its state depends on information transmitted by means of the information infrastructure.
- *Geographical dependency*: A geographic dependency 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 a failure in one or more near infrastructures.
- *Logical dependency*: Two infrastructures are logically dependent if their dependency is generated via control, regulatory, or other mechanisms that cannot be considered physical, geographical, or cyber.

The above categories have been further enriched in [5] by explicitly considering also the following:

- *Sociological dependency*: An infrastructure shows a sociological dependency when its operativeness is affected by the spreading of "disorder" related to human activities, that is, the emerge and diffusion of collective behaviors that have some negative impact on the capability of the infrastructure to correctly work.

The representation of human behavior within models is a challenging yet mandatory task. In fact the ability to take into account malicious behaviors, lack of coordination and cooperation among human operators, and sociological interactions and dynamics (such as strikes or the spread of an epidemy) will tremendously enrich the predictive ability of models. In [6], it is emphasized that, to correctly understand the behavior of interdependent infrastructures, it is mandatory to adopt a three-layered perspective:

- *Physical layer*: the physical component of the infrastructure, for example, the grid for the electrical network;
- *Cyber layer*: hardware and software components of the system devoted to control and manage the infrastructure, for example, Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS);
- *Organizational layer*: procedures and functions used to define activities of human operators and to support cooperation among infrastructures.

Notice that a similar kind of decomposition was used also to analyze the 2003 blackout in the United States and Canada [7]. Most of existing methodologies can be referred as *Holistic*, since each infrastructure is represented as a unique, monolithic entity. Among the others, the *Input–Output Inoperability Model* (IIM) [8] gained large attention. Within this class of models, however, the interactions between different infrastructures are modeled with an high level of abstraction, while the behavior of subsystems is masked. Such an high level of abstraction (and simplification) does not take into account the structure and the geographical extension of the infrastructures. Considering each infrastructure as an atomic entity represents a very crude simplification that does not take into account its geographical extension and its structure. There is, therefore, the need to adopt bottom-up approaches, as largely done when dealing with scarce or ill-defined macro-scale information, like in the field of bio-complexity.

Following the bottom-up philosophy, each infrastructure can be decomposed into a set of elementary interconnected components, taking into account both intra-infrastructure and cross-infrastructure dependencies and interdependencies. In order to obtain more insight on the behavior of interdependent infrastructures, a first step is to represent them as complex networks composed of similar basic elements (i.e., a network of distributed and interconnected generators may represent an electrical infrastructure), inspecting emerging behaviors generated by the interconnection of such elements [9,10,11,12]. The assumption of homogeneity, however, limits the applicability of these methodologies, since in real cases infrastructures are composed of highly heterogeneous subsystems; moreover, topological methods typically limit their scope to the geographical interaction of subsystems.

A step further is done by adopting *Simulative* perspective, focusing on a sophisticated representation of the isolated behavior of subsystems and then considering their interaction by means of simulation platforms and tools. Within this latter category, the most diffused is the *Agent-Based* approach [13,14], where infrastructures are decomposed into a set of interacting *software agents*, each with a dynamic and with heterogeneous level of abstraction.

In order to enhance the comprehension of highly interdependent scenarios, in [15,16], the agent-based perspective was further enriched, considering, at the same time, multiple and partly overlapping representations of the scenario (i.e., physical, functional, and global representations).

## 3 Holistic approaches

Holistic approaches (See Figure 1) are, generally speaking, very abstract, simplified, and strategic oriented. These frameworks can be setup quite easily; even if several important aspects are neglected (e.g., the geographical dispersion that characterize several infrastructures), they have the merit to be compact and understandable; moreover, these methods allow to represent several interdependent infrastructures at the same time, even if all the interaction is generally reduced to an abstract parameter, the inoperability.

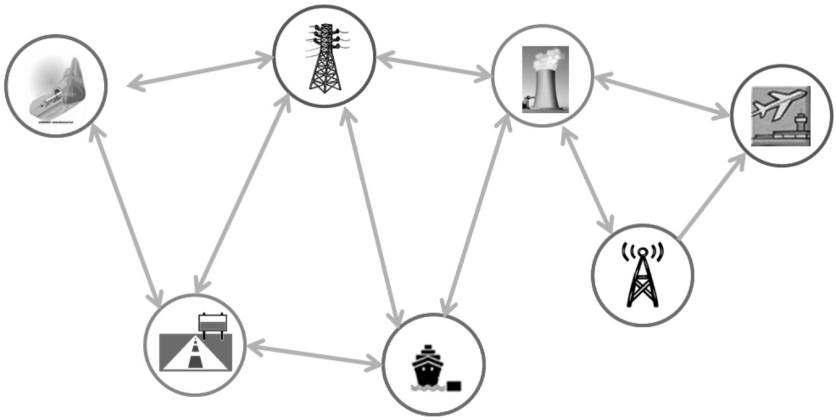

Figure 1: Holistic approaches. Within this framework infrastructures are considered as a whole, focusing on their high-level interaction.

Among the others the IIM model [8] and its further evolutions (for instance, the *Dynamic Input–Output Model* (D-IIM) [17], which considers the *dynamic* of the system, until an equilibrium is reached, or the *Multi-Regional IIM Model* (MR-IIM) [18], which allows to represent multi-sectoral and multiregional economic interdependencies) are widely diffused.

The main objective of the IIM model, introduced in [8,17] as an application of the economic theories of the Nobel Prize winner Wassily Leontief [19], is to represent within a simple framework the global effects of negative events in scenarios composed of highly interdependent infrastructures.

With a high level of approximation, the approach assumes that each infrastructure is modeled as an atomic 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 that require goods or services produced by the *i*-th one. These degradations may be further propagated to other infrastructures (cascade effect) and even exacerbate the situation of the *i*-th one due to the presence of feedback loops.

The model, based on economic data, analyzes how the effects of natural outages or terroristic attacks in one infrastructure may affect the others, highlighting cascading effects and intrinsic vulnerabilities. The main assumption, for this approach, is that “two companies with a large amount of economic interaction will have a similarly large amount of physical interdependency” [17].

The estimation of such interaction has been addressed in many different ways; however, the most diffused and reliable data sources (for the United States) are the Bureau of Economic Analysis (BEA) database of national Input–Output (I-O) accounts and the Regional Input–Output Multiplier System (RIMS II).

The BEA database provides a series of tables depicting the production and consumption of *commodities* (goods and resources) by various sectors in the

U.S. economy. These data are then combined to calculate the *Leontief technical coefficients*, which are used within the IIM framework.

In the original Leontief model, each industry is assumed to produce a single commodity; since this assumption is not realistic, the BEA considers different commodities for each industry and provides two different data matrices: the *industry by commodity* and the *commodity by industry* matrices [20]. These matrices, often referred as *make* and *use*, have to be composed to derive the I-O matrix [17,21].

Mathematically, IIM describes these phenomena on the basis of the level of inoperability associated to each infrastructure. The inoperability of the $i$-th infrastructure, at each time instant $k$, is represented by the variable $x_i \in [0,1]$, where $x_i = 0$ means that the infrastructure is fully operative, while $x_i = 1$ stands for complete inoperability. In a very general formulation, IIM model can be written as follows:

$$x(k + 1) = Ax(k) + c, \tag{1}$$

where $x$ and $c$ are the vectors composed, respectively, by the level of inoperability and by the external failure and $A$ is the influence matrix, that is, the matrix of the technical coefficient of Leontief. The element $a_{ij}$ of this matrix represents the fraction of inoperability transmitted by the $j$-th infrastructure to the $i$-th one or, in other terms, how much the inoperability of the $j$-th infrastructure influences the $i$-th infrastructure.

Although the IIM framework is very compact and elegant, and is able to model cascading effects, its high degree of abstraction does not allow to perform accurate analyzes on the real nature of dependencies; in fact such an approach considers only relations that involve whole infrastructures, while it is impossible to understand and represent the contribution of each subsystem. This latter aspect is fundamental, in order to address the huge complexity of geographically dispersed systems.

Moreover, the economic origin of IIM model represents a structural limitation: In fact, even if use/make matrices are considered, taking into account the production and consumption of multiple commodities for each infrastructure, only the economic value of such commodities is typically available. Although some attempts have been proposed to decompose infrastructures with a finer grain perspective and relate the Leontief coefficients to components or subsystems [13], it is difficult to retrieve exact quantitative data required to setup the model. In fact, IIM models are typically based on macro-economic data, which cannot be easily decomposed. An alternative, then, is to represent interdependency according to the sector-specific knowledge of operators, technicians, and stakeholders.

Anyhow, since each stakeholder has a limited knowledge of the interaction phenomena that may cross the boundary of the single infrastructure, there is the need to involve the different stakeholders and interact with them in order to correlate, compare, and encode their sector-specific knowledge. An attempt in such a direction has been done in [22], where IIM coefficients have been assessed by means of specific questionnaires and technical interviews. Another effective approach, introduced in [14] is the *Agent-Based IIM Model* (AB-IIM), where the production, consumption, and transmission of resources at low level was considered, providing interdependency matrices with a physical meaning.

## 4 Critical Infrastructures as Complex Systems

In the past century, the scientific community has been more and more devoted to decompose and analyze reality, assuming that complexity would be easily reduced if every elementary subsystem was perfectly known. Unfortunately, this will never happen; in fact, according to Aristotle's *Metaphysics*, "The whole is more than the sum of its parts." Indeed in many fields complexity arises when the *interaction* between elementary parts is considered. A *Complex System*, then, is a system composed of interconnected parts that as a whole exhibit one or more properties not obvious from the properties of the individual parts [23]. This characteristic is called *emergence*. Consider, for instance, the human brain, which is composed of a huge set of heavily interconnected neurons, or the ecosystem, whose behavior cannot be fully explained by considering only the isolated behavior of animals and plants.

Indeed, critical infrastructures show a number of structural and "behavioral" features that cannot be explained by considering isolated infrastructures or subsystems; such properties have been widely investigated in the past years [24,25,26,27,28]. The promise of these efforts is to unveil relevant insights on growth mechanisms, causes of vulnerability, dynamic behavior under perturbation, onset of emerging phenomena, and so on, even neglecting some peculiar characteristics.

According to the recent developments there are two aspects that, if properly analyzed, may allow to gain relevant insights on critical infrastructures:

- the study of *topological* properties of the graph representing the infrastructure and
- the study of *functional*, emerging behaviors and properties that arise when the different subsystem are considered as dynamically coupled systems, (See Figure 2) relying on some functional model able to reproduce the dynamic process (mainly transport of some entity, like electricity, data, vehicles, etc.) taking place on them.

### 4.1 Topological analysis

Topological analysis of critical infrastructures received a renewed interest after the pioneering works of Strogartz and Barabasi [9,10]. In these studies, they emphasized that many technological, social, and biological networks may evolve without any central authority, nevertheless showing peculiar structural patterns like *small world* and *scale free*, with immediate consequences on many properties and characteristics of the corresponding infrastructures.

Specifically, it has been shown that scale-free models, with few hubs (i.e., nodes with a high number of connections) and a poorly connected peripheries, show good

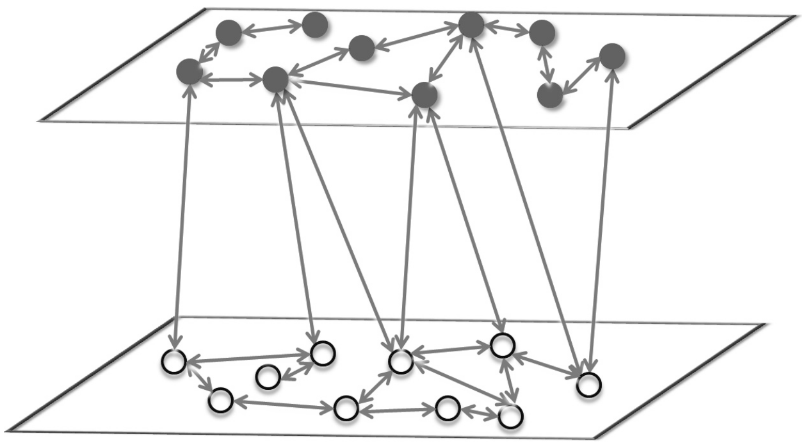

Figure 2: Topological approaches. Within this framework infrastructures are considered as networks composed of homogeneous elements, inspecting their topological properties (i.e., their resilience to node removal) or their functional behavior (i.e., the effect of node removal on the power flow).

resilience against accidental (or random) failures but are prone to deliberate attacks [29]. At the same time, the small-world property, which implies low average path lengths with respect to the number of nodes in the network, can lead to a very fast propagation of pandemic events, carried out by viruses, failures, or ill-services.

These approaches, in their most simple formulation, assume that each infrastructure is composed of a set of identical elements (generally represented as nodes on a graph) and infer dependencies analysis assuming some sort of relationship existing among nodes belonging to different networks [12,30,31].

Within this framework the degree of interdependency is generally assessed by taking into account structural properties of the overall graph (e.g., connectivity, betweennes, minimal path length, etc.), either in normal or critical conditions (i.e., after the disruption of some nodes or edges) [25]. These approaches, therefore, operate with an ON/OFF assumption, that is, each node either is fully working or it is completely out of work.

Topological analysis is quite easy to setup, since only the topologies of the different infrastructures considered are required.

However, although this approach is very effective in the case of two infrastructures characterized by a single predominant dependency mechanism (e.g., physical), the generalization to multiple infrastructures and dependency mechanisms is absolutely not straightforward.

Indeed these methods assume physical couplings as the primary source of interdependency while, especially for highly technological and automated infrastructures, cyber dependency is not considered.

Moreover, it is worth to notice that large technological infrastructures do not often show a clear "scale-free" structure, especially due to technological constraints that limit the growth of node's degrees [32]. As a consequence, results about robustness and resilience, based on the assumption of pure scale-freeness, cannot be directly applied in many technological contexts, leaving the issues related to structural vulnerability to be differently evaluated on each case [25].

Finally, in several cases, for example, for 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 (i.e., because of the presence of buffers, batteries, and multiple paths).

To overcome the above issues, it has been suggested to consider also network dynamics, and to this end they superimpose to the topological structure some form of flux dynamic models [33].

### 4.2 Functional analysis

Unlike the structural analysis, functional analysis of Critical Infrastructure is an hard task. Besides the intrinsic complexity of the topic, that is due to the lack of accurate and complete functional data of the infrastructures, often treated as confidential and classified by the stakeholders.

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 have appeared. The results reported in the literature emphasize how structural and functional vulnerability are substantially blandly correlated concepts that capture different properties, that is, two networks should be strongly coupled from the structural point of view, and in the same time lightly coupled when considering the functional properties and vice versa. Unfortunately, there are no final indications able to emphasize which one of these properties is the most relevant to explain those apparent incoherences.

In order to overcome such limitations, some simplifying hypothesis are generally assumed, enabling the development of "simpler" functional models, still able to capture the basic features of the networks but disregarding the most complex effects related to the exact technological implementations.

Then, the main aim of functional analysis is to evaluate the effects on the flows existing on the different networks and induced by simple topological perturbations. However, in order to perform a functional vulnerability assessment it is not sufficient to acquire information about the topological structure of the network, but there is also the need to model the characteristics of the fluxes and their specific parameters. This introduces several degrees of freedom into the model that may drive to erroneous conclusions.

Kurant and Thiran [34] have analyzed a system composed of several homogenous networks (i.e., of similar nature) interacting by exchanging loads, while in [35] there is an attempt in the direction of studying heterogeneous inter-dependent networks (i.e., formed by infrastructures of different nature), showing that the coupling makes the system more susceptible to large failure. A similar result has been reported in [30] where statistical mechanics and mean field theory are used to extrapolate steady state solutions in response to removal of a fraction of nodes. In [36] 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 [31] 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 [37] where five types of infrastructure interdependencies are presented and incorporated into a network flow framework and tested with reference to the lower Manhattan region of New York. In [11,33] the interconnection properties of an electric grid and a Telecommunications (TLC) network that mimic the Italian situation are studied, relying on the *DC Power Flow Model* [38] to represent the electric power flow and considering also the packet routing in the TLC network. It has been shown that the cut of one or more links induces a change of the power flow distributions over the network. However, exploiting this simple model, it results that, for several different cuts, a solution is inhibited by the physical constraints imposed by the model itself. In other terms, due to overload conditions or unbalancing situations, the electric grid is no longer able to supply energy, implying the presence of possible blackouts if any corrective action is taken. Such a kind of dramatic consequences do not comply with the real data (and the common sense). Indeed, in order to prevent such catastrophic conditions, the operators of the electric networks continuously perform corrective and adjustment actions to limit the insurgence of blackouts. Hence, in order to take into account such mechanisms of self-tuning, there is the need to consider also some *re-dispatching* strategies that, miming the typical policies adopted by electrical operators, enable to modulate produced and dispatched powers [11].

The key aspect of such methods, therefore, is that complex behaviors in highly interdependent scenarios can be evaluated by focusing on the interaction among sets of simple and well-known elementary components; the true weak point, however, is that only homogeneous subsystems are typically considered while, in real scenarios, infrastructures are composed of highly heterogeneous subsystems, each characterized by a particular behavior. Moreover, it is not easy to extend such methodologies in order to consider the interaction among multiple and heterogeneous infrastructures.

## 5 Simulative approaches

In order to overcome the limitations of a mere topological framework, *simulative* approaches are introduced as methods focused on the analysis of the dynamic of each single component; then, the interdependency existing among the infrastructures is evaluated considering the interaction among such subsystems (See Figure 3).

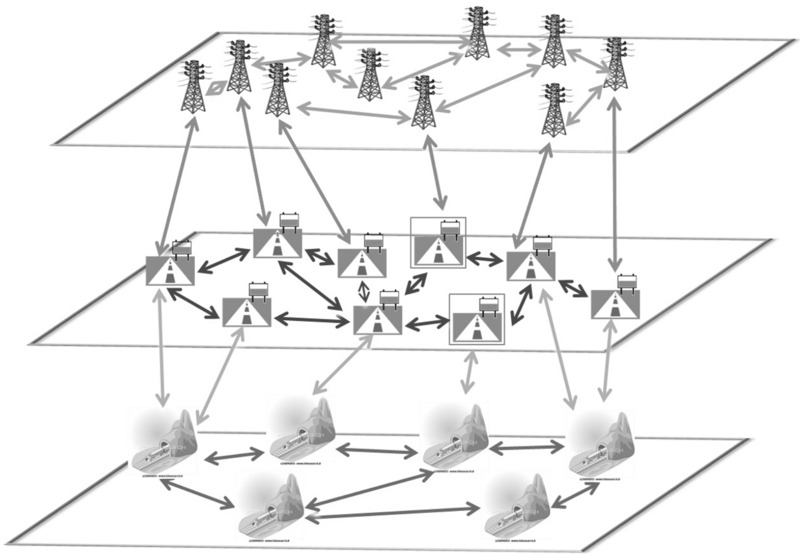

Figure 3: Simulative agent-based approaches. Infrastructures are decomposed into a set of software agents or entities, focusing on their behaviors; then the interconnection among these entities is considered, taking into account both intra-domain and inter-domain dependencies.

Generally, these approaches are quantitative in nature and operative oriented. In fact, it is possible to consider a continuous level of degradation in the component functionalities and the concurrent presence of several types of phenomena (like the absence of resources, external failures, and internal dynamics).

Simulative approaches, therefore, are mainly devoted to provide an answer to the following questions:

- What are the consequences of attacks, failures, incidents, and natural disasters on the different infrastructures existing in a given area in terms of national security, economic impact, public health, and conduct of government?
- The failure of which elements, once affected by failures, have the largest impact in the areas, taking into account both direct consequences and those induced by domino effects?

These methods, then, exploit the power of simulation platforms in order to estimate the impact of a given failure into a scenario composed by several heterogeneous and interdependent infrastructures (see, among the others [39,40,41]).

In order to deploy a simulation scenario, the researchers have to acquire/define:

- the internal model of each single component of the different infrastructures;
- the intra-dependency model, that is, how components interact inside each single infrastructure; and
- the interdependency model, that is, how components belonging to different infrastructures interact.

A variety of simulation have been developed in these years to analyze the operational aspects of individual infrastructures (e.g., load flow and stability programs for electric power networks, connectivity and hydraulic analyzes for pipeline systems, traffic management models for transportation networks). In addition, simulation frameworks that allow the coupling of multiple, interdependent infrastructures are beginning to emerge [39,40,41,42]. The Idaho National Lab conducts an interesting overview of the different approaches and tools used for the modeling and the simulation of interdependent infrastructures [39]. Another useful review about simulation tools is those performed inside the Design of an Interoperable European Federated Simulation Network (DIESIS) project [43].

Unfortunately, the set up of such simulators is a hard challenge; in fact a huge amount of detailed data is required to tune the models, and often, subjective hypothesis are introduced by the modelers, influencing the correctness of the solutions.

One of the most promising patterns for the analysis of the interdependencies between complex networks is the agent-based paradigm [44]. The fundamental idea that drives these models is that the complex behavior is the fruit of the interactions between autonomous and elementary individuals, which operate on the basis of simple rules, and that interacting together makes the collective behavior of the system emerge.

Nevertheless, in order to provide more insight on the overall System of Systems, *Multilayer* approaches have recently been introduced [15,16,45] as an extension of the agent-based paradigm able to consider, at the same time, multiple and partly overlapping representations of the same scenario, in order to capture the most important behaviors and dynamics from different perspectives.

## 5.1 Agent-based approaches

Within the agent-based framework, the behavior of an interdependent infrastructure is analyzable by resorting to a bottom-up approach, which models the whole system starting from the (local) behavioral knowledge of single components and then taking into account the interaction among these subsystems. Infrastructures, then, are decomposed into a set of interconnected *software agents* or *entities* [44].

A good example of such simulators is EPOCHS [40], which is designed to analyze interactions between the electric grid and telecommunications networks. Another example is SimCIP, which is being developed under the IRRIIS Project [42].

The most challenging issue is how to encode different, vague, and often contradictory information sources; a probabilistic approach seems not feasible, since here information is vague and linguistic, rather than stochastic.

In order to overcome these limitations, in [41] the Critical Infrastructure Simulation by Interdependent Agents (CISIA) simulator was introduced, as an

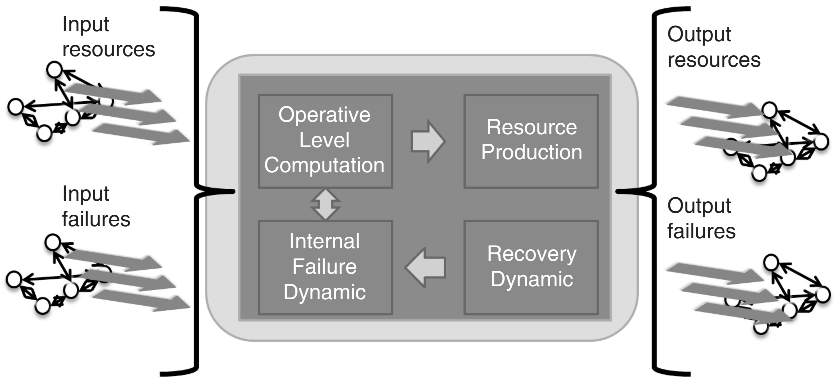


Figure 4: Detail of an entity within CISIA framework. The whole model is composed of $n$ entities belonging to $N$ different infrastructures, which exchange $m$ different types of resources and $p$ different typologies of failures, belonging to $M$ and $P$ networks, respectively; each of these networks is used to take into account a specific concept of proximity.

agent-based framework where the behavior of entities and their interaction are modeled by means to fuzzy logic and fuzzy inference. Figure 4 represents the detail of an entity; within this framework the exchange of different classes of resources and failures is explicitly modeled. Besides computing the operative level, the behavior of each entity can be influenced by internal failures; moreover, the severity of failures can be influenced by the operational conditions of the entity and by the presence of recovery/restoration mechanisms.

Within such an approach, the exchange of resources and the spread of failures were represented, also taking into account the delays and dissipations due to the transportation of resources and failures and peculiar internal dynamics of the different agents. This approach has been successfully tested on a realistic scenario on a regional scale, composed of 233 entities belonging to 7 infrastructures and exchanging 43 quantities (of which 13 failures) by means of 13 networks for a total of about 844 links.

### 5.2 Multilayer approaches

As exposed above, limiting the scope to the interaction among subsystems may lead to crude approximations [6], in fact, besides being a set of interconnected components, an infrastructure is characterized by emerging functional behaviors and is greatly influenced by human behavior and sociological phenomena. When dealing with complex, highly interdependent scenarios, a single perspective may be reductive, as stressed in [46].

An effective approach, then, is to take into account multiple representations of the same reality, each devoted to highlight a particular class of phenomena.

In [15], critical infrastructures are represented according to three hierarchical layers:

- *Micro-level*: represents the physical components that constitute the functional elements of an infrastructures (i.e., electrical equipments, gas valves, etc.),
- *Meso-level*: represents an infrastructure network at the system level (i.e., network nodes and links, power generators and loads, etc.),
- *Macro-level*: represents the territory or zone that depend on the service provide by the infrastructure.

Within this framework, each level is considered as a nested subsystem, which can be analyzed independently. Moreover, the propagation of effects is assumed to spread from the micro- to the macro-level, neglecting downstream consequences and focusing on the effect of outages and failures on higher levels.

A more sophisticated approach is the *Mixed Holistic–Reductionistic* (MHR) framework, introduced in [45] and refined in [16], where three not mutually exclusive layers were considered:

- *Reductionistic layer*: Infrastructures are decomposed, following the agent-based perspective, into a set of interrelated subsystems. Physical behaviors and dynamics are encoded at this level. Moreover, it is possible to represent the spreading of failures with a physical meaning (i.e., a fire blast).
- *Service layer*: Infrastructures are decomposed according to a functional perspective, considering entities able to provide aggregate resources or services. At this level, it is possible to represent infrastructure functionalities provided to the final customers (i.e., [GSM], VoIp services) or consider intermediate services and behaviors required for the correct operativeness of the same or different infrastructures (i.e., power network reconfiguration, message dispatching, etc.). At this level, it is possible to represent higher level failures (i.e., computer viruses, sociological failures), which are not easy to represent at lower level.
- *Holistic layer*: Analogously to IIM model, at this level the global interaction among infrastructures is analyzed. At this level, it is possible to model complex phenomena, for example, a strike, which are difficult to represent at the other levels.

Starting from previous experience of CISIA simulator, the MHR–CISIA [16] tool was developed, in order to take into account the above three layers, considering both intra-layer and inter-layer interactions. Such an approach has been used within the MICIE European Project [47] as the modeling framework for the definition of a distributed online risk predictor.

## 6 Conclusions

In this chapter, the most diffused approaches for the modeling and simulation of interdependent critical infrastructures have been reviewed.

Starting from a pure holistic approach, where infrastructures are modeled with an high level of abstraction, and taking into account economic interaction, infrastructures are subsequently decomposed into networked sets of homogeneous subsystems, considering their topological properties or even the flow dynamic under critical conditions. However, topological approaches are not easily extensible to multiple, highly heterogeneous scenarios; in order to overcome these limitations, simulative approaches are introduced. Initially, infrastructures are decomposed into sets of software agents, focusing on their internal behavior; then the interaction among these subsystems are inspected. Finally, multilayered models try to capture interdependency phenomena by considering multiple agent-based layers, with a physical, functional, or systemic perspective.

Increasing the complexity of models may lead to more sophisticated and predictive representations; however, as the level of detail increases, it is hard to retrieve adequate quantitative data. Moreover, each stakeholder has a good knowledge of its infrastructure and subsystems, while the comprehension of cross-infrastructure dependencies is generally poor and unclear.

There is, therefore, the need to define adequate data-collection procedures, in order to cope with uncertain, incomplete, and often contradictory information.

## References


[1] M. Suter & E. Brunner, *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, 2008.

[2] E.U. Commission, *Green Paper on a European Programme for Critical Infrastructure Protection COM(2005)576*, Commission of the European Communities, Brussels, 2005.

[3] S. Rinaldi, J. Peerenboom, & T. Kelly, "Identifying Understanding and Analyzing Critical Infrastructure Interdependencies," *IEEE Control System Magazine*, vol. 21, pp. 11–25, 2001.

[4] R. Setola, "How to Measure the Degree of Interdependencies among Critical Infrastructures," *International Journal of System of Systems Engineering*, vol. 2, no. 1, 2010.

[5] S. De Porcellinis, R. Setola, S. Panzieri & G. Ulivi, "Simulation of Heterogeneous and Interdependent Critical Infrastructures", *International Journal of Critical Infrastructures*, vol. 4, n 1/2, pp. 110–128, 2008.

[6] R. Macdonald & S. Bologna, "Advanced Modelling and Simulation Methods and Tools for Critical infrastructure Protection," *ACIP project report*, 2001.

[7] U.S. and Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," 2004, http://reports.energy.gov.

[8] Y. Haimes & P. Jiang, "Leontief-Based Model of Risk in Complex Interconnected Infrastructures," *Journal of Infrastructure Systems*, vol. 7, no. 1, pp. 1–12, 2001.

[9] D. J. Watts & S. H. Strogartz, "Collective Dynamics of Small-World Networks," *Nature*, vol. 393, pp. 440–442, 1998.

[10] H. Jeong, S. P. Mason, A. L. Barabasi, & Z. N. Oltvai, "Lethality and Centrality in Protein Networks," *Nature*, vol. 411, pp. 41–42, 2001.

[11] S. De Porcellinis, L. Issacharoff, S. Meloni, V. Rosato, R. Setola, & F. Tiriticco, Modelling Interdependent Infrastructures Using Interacting Dynamical Models. *International Journal of Critical Infrastructures*, vol. 4, no. 1/2, pp. 63–79, 2008.

[12] L. Duenas-Osorio, J. I. Craig, B. J. Goodno, & A. Bostrom, "Interdependent Response of Networked Systems," *Journal of Infrastructure Systems*, vol. 13, no. 3, pp. 185–194, 2007.

[13] R. Setola, S. De Porcellinis, & M. Sforna, Critical Infrastructure Dependency Assessment Using the Input–Output Inoperability Model, *International Journal on Critical Infrastructure Protection*, vol. 2, no. 4, pp. 170–178, 2009.

[14] G. Oliva, S. Panzieri, & R. Setola, "Agent-Based Input–Output Interdependency Model," *International Journal on Critical Infrastructure Protection*, vol. 3, no. 2, pp. 76–82, 2010.

[15] C. Di Mauro, S. Bouchon, C. Logtmeijer, R. D. Pride, T. Hartung, & J. P. Nordvik, "A Structured Approach to Identifying European Critical Infrastructures," *International Journal of Critical Infrastructures*, vol. 6, no. 3, pp. 277–292, 2010.

[16] S. De Porcellinis, G. Oliva, S. Panzieri, & R. Setola, A Mixed Holistic–Reductionistic Approach to Model Interdependent Infrastructures, *Critical Infrastructure Protection IV*, M. Papa and S. Shenoi eds., vol. 311, pp. 215–227, Springer, Boston, 2009.

[17] Y. Haimes, B. Horowitz, J. Lambert, J. Santos, C. Lian, & K. Crowther, "Inoperability Input–Output Model for Interdependent Infrastructure Sectors I: Theory and Methodology," *Journal of Infrastructure Systems*, vol. 11, no. 2, pp. 67–79, 2005.

[18] K. G. Crowther & Y. Y. Haimes, "Development of the Multiregional Inoperability Input–Output Model (MRIIM) for Spatial Explicitness in Preparedness of Interdependent Regions," *Systems Engineering*, vol. 13, no 1, pp. 28–46, 2010.

[19] W. Leontief, *The Structure of the American Economy 1919–1939*. Oxford University Press, Oxford, 1951.

[20] J. Guo, A. M. Lawson, & M. A. Planting, "From Make-Use to Symmetric I-O Tables: An Assessment of Alternative Technology Assumptions," *Proceedings of the 14th International Conference on Input–Output Techniques*, Montreal, Canada, October 10–15, Bureau of Economic Affairs, U.S. Dept. of Commerce, Washington DC, 2002.

[21] E. Kujawski, "Multi-Period Model for Disruptive Events in Interdependent Systems," *Systems Engineering*, vol. 9, no. 4, pp. 281–295, 2006.

[22] R. Setola, S. De Porcellinis, & M. Sforna, "Critical Infrastructure Dependency Assessment Using the Input–Output Inoperability Model," *International Journal of Critical Infrastructure Protection,* vol. 2, no. 4, pp. 170–178, 2009.

[23] C. Joslyn & L. Rocha, "Towards Semiotic Agent-Based Models of Socio-Technical Organizations," *Proceedings of the Conference on AI, Simulation and Planning in High Autonomy Systems Conference*, Tucson, AZ, pp. 70–79, 2000.

[24] R. Albert, I. Albert, & G. L. Nakarado, "Structural Vulnerability of the North American Power Grid," *Physical Review E*, vol. 69, no. 2, pp. 025103(R), 2004.

[25] P. Crucitti, V. Latora, & M. Marchiori, "A Topological Analysis of the Italian Electric Power Grid," *Physica A*, vol. 338, no. 1–2, pp. 92–97, 2004.

[26] R. Pastor-Satorras, A. Vazquez, & A. Vespignani, "Dynamical and Correlation Properties of the Internet," *Physical Review Letters*, vol. 87, no. 25, pp. 276–282, 2001.

[27] L. Issacharoff, S. Bologna, V. Rosato, G. Dipoppa, R. Setola, & F. Tronci, "A Dynamical Model for the Study of Complex System's Interdependence," in *Proceedings of the International Workshop on Complex Network and Infrastructure Protection (CNIP'06)*, Rome, March 28–29, pp. 276–282, 2006.

[28] F. Tiriticco, S. Bologna, & V. Rosato, "Topological Properties of High-Voltage Electrical Transmission Networks," *Electric Power Systems Research*, vol. 77, no. 2, pp. 99–105, 2006.

[29] R. Albert & A. L. Barabasi, "Statistical Mechanics of Complex Networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

[30] B. A. Carreras, D. E. Newman, P. Gradney, V. E. Lynch, & I. Dobson, "Inter-dependent Risk in Interacting Infrastructure Systems," *Proceedings of the 40th Hawaii International Conference on System Sciences*, Hawaii, January 3–6, 2007.

[31] N. K. Svendsen & S. D. Wolthusen, "Multigraph Dependency Models for Heterogenous Critical Infrastructures," *Proceedings of the First Annual IFIP TC 11.10 International Conference on Critical Infrastructure Protection*, Hanover, NH, March, pp. 337–350, 2007.

[32] L. A. N. Amaral, A. Scala, M. Barthelemy, & H. E. Stanley, "Classes of Small-World Networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 97, no. 21, October 10, pp. 11149–11152, 2000.

[33] V. Rosato, L. Issacharoff, S. Meloni, F. Tiriticco, S. De Porcellinis, & R. Setola, "Modelling Interdependent Infrastructures Using Interacting Dynamical Models," *International Journal of Critical Infrastructures*, vol. 4, no. 1/2, pp. 63–79, 2008.

[34] M. Kurant & P. Thiran, "Layered Complex Networks," *Physical Review Letters*, vol. 96, no. 13, 2006.

[35] D. E. Newman, B. Nkei, B. A. Carreras, I. Dobson, V. E. Lynch, & P. Gradney, "Risk Assessment in Complex Interacting Infrastructure Systems, HICSS 05," *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, IEEE Press, Big Island, HI, January 3–6, p. 63, 2005.

[36] N. K. Svendsen & S. D. Wolthusen, "Analysis and Statical Properties of Critical Infrastructure Interdependency Multiflow Models," *Proceedings from the Eighth Annual IEEE SMC Information Assurance Workshop, United States Military Academy*, West Point, NY, June, pp. 247–254, 2007.

[37] E. E. Lee, J. E. Mitchell, & W. A. Wallace, "Restoration of Services in Inter-dependent Infrastructure Systems: A Network Flow Approach," *IEEE Trasactions on Systems, Man and Cybernetics—Part C*, vol. 37, no. 6, pp. 1303–1317, 2007.

[38] P. A. J. Wood, & B. F. Wollenberg, *Power Generation, Operation and Control*, John Wiley, New York, 1984.

[39] P. Pederson, D. Dudenhoeffer, S. Hartley, & M. Permann, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idahho National Laboratory, Idaho Falls, ID, 2006.

[40] K. Hopkinson, K. Birman, R. Giovanini, D. Coury, X. Wang, & J. Thorp, EPOCHS: Integrated Commercial Off-the-Shelf Software for Agent-Based Electric Power and Communication, *Proceedings of the Winter Simulation Conference*, New Orleans, LA, December 7–10, pp. 1158–1166, 2003.

[41] S. De Porcellinis, S. Panzieri, & R. Setola, "Modelling Critical Infrastructure via a Mixed Holistic Reductionistic Approach," *International Journal of Critical Infrastructures*, vol. 5, no. 1/2, pp. 86–99, 2009.

[42] IRRIIS Consortium, The IRRIIS European Integrated Project, Fraunhofer Institute for Intelligent Analysis and Information Systems, Sankt-Augustin, Germany (www.irriis.org).

[43] EU project DIESIS (Design of an Interoperable European Federated Simulation Network for Critical InfraStructures), http://www.diesis-project.eu/.

[44] T. Brown, W. Beyeler, & D. Barton, "Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems," *International Journal of Critical Infrastructures*, vol. 1, no. 1, pp. 108–117, 2004.

[45] S. Panzieri, S. De Porcellinis, & R. Setola, "Model critical infrastructure via a mixed holistic–reductionistic approach," *International Journal on Critical Infrastructures*, vol. 5, pp. 86–99, 2009.

[46] F. Flammini, N. Mazzocca, C. Pragliola, & V. Vittorini, A Study on Multiformalism Modelling of Critical Infrastructures, *Proceedings of the 3rd International Workshop on Critical Information Infrastructures Security* (CRITIS 2008), LNCS 5508, Rome, Italy, October 13–15, 2008, pp. 336–343, 2009.

[47] MICIE European Project, http://www.micie.eu.