We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Resilience in Critical Infrastructures: The Role of Modelling and Simulation

Chiara Foglietta and Stefano Panzieri

Abstract

Resilience and risk are fundamental concepts for critical infrastructure protection, but it is complex to assess them. Modelling critical infrastructure interdependency helps in evaluating the resilience and risk metrics. We propose the MHR approach as a road-map to model infrastructures and it is implemented using CISIApro 2.0. MHR suggests considering three different layers in each infrastructure: holistic, service and reductionist agents. In this chapter, this framework has been tested in a scenario made of a modern telecommunication network, a hospital ward and a smart factory. The scenario takes into account cyber attacks and their consequences on the components, services and holistic nodes. The proposed framework is under validation within the EU H2020 RESISTO project with good results and in various test-beds.

Keywords: resilience metric, risk management, critical infrastructure modelling, simulation

1. Introduction

Critical Infrastructure is an evolving concept. Critical infrastructure was linked to aging public works in the 1980s: the National Council on Public Works Improvement in 1988 focused on public sector infrastructure. In the 1990s, infrastructure was redefined in terms of national security as a consequence of increased international terrorism. The number of critical infrastructure sectors in the National Infrastructure Protection Plan [1] has been enlarged to 17 since 9/11: it includes agriculture and food systems, the defense-industrial base, electricity systems, public health and health care facilities, national monuments, banking and financial systems, drinking water systems, chemical services, commercial buildings, dams, emergency services, nuclear power plants, information technology networks, telecommunications systems, postal and shipping services, transportation systems, and government facilities. Critical infrastructure is identified in Europe under the term "essential services" [2].

Shifting the concept of critical infrastructures has led to more flexibility and adaptability. The sophistication of an already complicated field, on the other hand, is increased, creating more confusion and more doubts. The definition of "lifeline system", [3] was then established by some researchers to assess the efficiency of large, geographically distributed networks during crises caused by adverse events,

such as natural disasters or cyber-attacks. Lifelines are classified into six major systems: electricity, gas and liquid fuels, telecommunications, transportation, waste management, and water provision. The economic well-being, security, and protection of our lives are closely related to those systems. Thinking of critical infrastructure across the sub-set of lifelines helps to simplify features common to important support structures and to enhance the performance of large networks, offering visibility into the technical challenges.

Lifeline systems, mostly on the basis of physical proximity and operational interaction, are interdependent. Cables and pipes are placed alongside each other in crowded area, resulting in an elevated risk due to proximity. Damage to one infrastructure component, such as an electrical cable, will easily ripple into damage to adjacent components, such as telecommunications cables and gas mains, with system-wide implications.

Lifeline systems are dependent on each other. Electric power networks, for example, supply electricity for pumping stations, storage facilities, and equipment control for transmission and distribution systems for oil and natural gas. Oil provides fuel and lubricants for generators, and natural gas provides energy for generating stations, compressors, and storage, all of which are required for the operation of electric power networks.

In the Merriam-Webster Dictionary, resilience is defined as "the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress" [4]. Definitions vary slight, but all of them relate the principle of resilience to physical stress recovery.

A notable change from securing critical infrastructures to ensuring that communities are resilient has taken place following Hurricane Katrina. Furthermore, the concept of resilience is evolving, as the idea of critical infrastructures. In its present form, a society's resilience is an overarching attribute that reflects the degree of community preparedness and the ability to respond to a crisis and rebound from it. Since lifelines are intimately linked to the economic well-being, security, and social fabric of a community, community resilience is closely related to the initial strength and gradual recovery of lifelines.

Debate over the concept of resilience is likely to persist, and refinements and elaborations of the term are to be expected. A framework for defining resilience has been suggested by the Multidisciplinary Center for Earthquake Engineering Research (MCEER) [5]. Resilience for both physical and social systems can be conceptualized as having four infrastructural qualities:

- Robustness: the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.

- Redundancy: system property that under stress allows for alternate solutions, decisions, and substitutions.

- Resourcefulness: the capacity to coordinate needed assets and services in crises.

- Rapidity: the speed at which disruption can be overcome and safety, services, and financial stability restored.

As shown in **Figure 1**, an infrastructural performance, such as robustness, $Q(t)$, can be visualized as a percentage that varies with time. For buildings, $Q(t)$ may be the percentage of structural or functional integrity. For lifelines, $Q(t)$ may be the percentage of customers that successfully receive power or drinking water. Prior to a natural hazard, severe accident, terrorist act, or a general disruption, $Q(t)$ is at 100

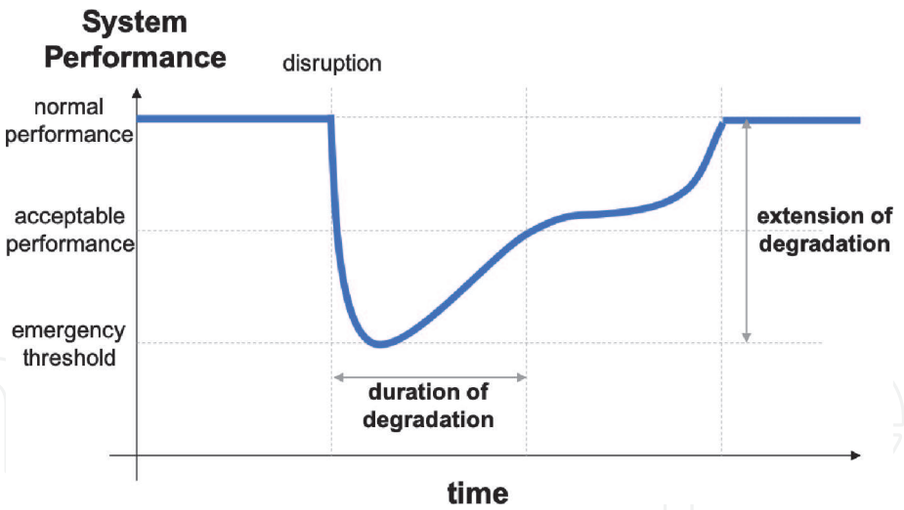


Figure 1.
The resilience profile.

percent; in picture is defined as normal performance. If the system is fully robust, it remains at 100 percent even during disruptions. Total loss of service results in 0 percent of $Q(t)$. If system disturbance occurs at time t_0, in response to, for example, an earthquake or hurricane, damage to the infrastructure may reduce the performance to less than 100 percent, the emergency threshold. Level of service, as reflected by the robustness of the system, is a function of the probability and consequences of damage. Robustness is restored over time; at time t_1, the system is returned to its original capacity. We called "duration of degradation" the time for the system to bounce back to an acceptable performance.

For a community or an infrastructure, the loss of resilience, R, can be measured as the expected loss in quality (probability of failure) over the time to recovery, $t_1 - t_0$. Thus, mathematically, R is defined as:

$$R = \int_{t_0}^{t_1} Q(t)dt \tag{1}$$

The resilience indicator, R, is a simple measure for quantifying resilience. In [5], additional mathematical developments of this notion cover the probabilistic and multidimensional aspects of resilience.

1.1 Contributions

The modeling method used in this chapter is based on the methodology of Mixed Holistic Reductionist (MHR), where each infrastructure is divided into components (reductionist layer), services (service layer) and holistic nodes (holistic layer). The MHR approach is a guideline on how we can decompose each infrastructure and how we can define the interconnection among the different components. It also allows the identification of the right abstraction level due to the available information.

The agent-based simulator, called CISIApro 2.0, is then used to implement this approach. This simulator presents the consequences of adverse and positive events in an interdependent scenario. In real-time, this simulator runs connected to a SCADA (Supervisory Control And Data Acquisition) control center to receive current information on faults and linked to an Intrusion Detection System (IDS) to acquire actual threats and on-going cyber-attacks. CISIApro 2.0 integrates heterogeneous data to improve the situational awareness of operators and their

decision-making process. This version of the simulator has been improved considering the telecommunication features. Specifically they are:

- Elements with multiple services
- Dynamic links
- Routing links
- Propagation models for ring topologies
- Continuous and discrete dynamics simulation inside the agents
- The possibility of co-simulating external dynamics
- The ability of revoke services

1.2 Organizations

This chapter is composed of the following sections: Section 2 analyses the idea of risk and resilience; Section 3 reviews the literature on critical infrastructures simulator; Section 4 presents the MHR approach while the simulator CISIApro 2.0 is described in Section 5; a telecommunication case study is summarised in Section 6; conclusions and future works are in Section 7.

2. The concepts of risk and resilience

The concepts of risk and resilience are similar and generally closely linked: improving the system's resilience requires reducing risk. Risk is commonly structured in terms of preparedness, mitigation measures, reaction capabilities, and recovery processes; anticipation, absorption, adaptation and recovery are the typical components of resilience.

Owners and operators can improve the resilience of critical infrastructures by specific operations: withstanding specific threats, reducing or mitigating potential impacts, returning to normal operations if such degradation occurs. A resilience methodology includes increasing preparedness for an incident, implementing redundancy to mitigate the effects of an incident, and strengthening the coordination and execution of response and recovery procedures, for emergency action and business continuity.

There are five main steps in the resilience cycle: prepare, prevent, protect, response and recover. The resilience cycle must consider the consequences of interdependencies among critical infrastructures. The tool we present in this chapter, called CISIApro 2.0, aims to assess the consequences of adverse events on critical infrastructures in terms of components, services and also holistic agents. CISIApro 2.0 usually helps the operators in the recovery phase, knowing which are the possible consequences of actual adverse events.

The Department of Homeland Security (DHS) defines risk as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences" [6]. Thus, risk is historically characterized as a function of three elements: the threats to which an asset is susceptible, the vulnerabilities of the asset to the threat, and the consequences potentially generated by the asset's deterioration.

Threat is a "natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property" [6]. Sometimes the term hazard, which can be defined as a "natural or man-made source or cause of harm or difficulty" [6], is used instead of threat. However, a "hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed" [6]. Vulnerability is a "physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard" [6]. Consequences are the "effects of an event, incident, or occurrence" [6].

The challenge is to determine where and how resilience integrates into risk assessment as risk is a feature of threats and hazards, weaknesses, and consequences. Resilience, as defined by DHS, is the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions" [6]. The DHS lexicon also states that "Resilience can be factored into vulnerability and consequence estimates when measuring risk" [6]. Therefore, the resilience will have an effect on both vulnerability and consequences.

On the basis of these characteristics, it is possible to develop specific indicators and metrics to assess the risk to an organization or an infrastructure. Considering a threat or hazard (man-made or natural), the vulnerability and resilience of an organization will impact the potential consequences of an event. The interaction between the elements of risk is complex and made more so when one considers the transfer of risk between assets in the case of a threat by an intelligent adversary.

3. Literature review on modelling interdependency

In literature, three main methodologies for the modelling approaches of critical infrastructure modelling are presented: agent-based simulation, input–output analysis and network modelling. Please refer to [7] for heterogeneous and/or unclassified approaches.

Each infrastructure is considered by agent-based simulations to be a complex adaptive structure, consisting of agents representing single aspects of the infrastructure itself. Different agents can be modelled at different degrees of abstraction based on the proposed level of resolution modelling. The primary benefit of agent-based simulation is the ability to establish synergistic behaviors as agents begin to work together [8].

The second method is based on the economic theory of Input–Output proposed by Leontief in the early 1930s, but later adapted to modelling infrastructures. Haimes and Jiang developed the linear input–output inoperability model (IIM) to research the impact of interdependencies on the inoperability of interconnected networked systems [9]. The key benefit of the IIM and its improvements is that the suggested solution is simple and flexible. IIM is usually confined to the financial costs of interdependencies.

In recent years, researchers have investigated new approaches to interdependency modelling of infrastructures. The most promising technique is based on graph and network theory. This approach uses abstract graphs made of nodes and arcs to describe infrastructures, representing links between components within infrastructures. The key benefit is to leverage closed form expressions and numerical simulations to characterise their topology, performance and uncertainty.

4. Mixed Holistic Reductionist (MHR) approach

In this chapter, we propose an already applied approach, for helping during the modelling phase. To maximize the benefits of holistic and reductionist approaches,

the Mixed Holistic Reductionist (MHR) [10] methodology was developed. The key goal of MHR approach is to provide a potential road-map to model critical infrastructures and their interdependencies properly.

In holistic modeling, infrastructures are seen as specific agents with defined boundaries and functional properties, creating a global and overall analysis. The purpose of presenting an infrastructure as a single element is to define the various infrastructures and their geographical extent. The volume of data needed for modeling activities is very limited at this stage and can be found in public data-sets.

In the other hand, to better appreciate the overall infrastructure, the reductionist approach stresses the need to thoroughly understand the roles and behaviours of individual components. The reductionist approach drills down to each component in terms of inputs and outputs. At this level of abstraction is easy to find dependencies between equipment and single components.

Various levels of analysis are required in modelled systems and their boundaries are lost in the event of complex case studies. For the MHR model, either a top-down or bottom-up approach might see relationships between infrastructures at different levels. The other key benefit is to model infrastructures at at multiple complexity levels, taking into account the quantity of data available.

The connection point between the two abstraction levels, i.e. holistic and reductionist approaches, is the quality of services (in the following, abbreviated as "service") which is a key element for operators. This layer describes functional relationships between components and infrastructure at different levels of granularity. Services to clients and to other interconnected infrastructures are specifically treated in MHR as a middle layer between holistic and reductionist agents.

The MHR allows us to reach the right level of detail with minimal data and collected information. Some important considerations can be summarised in the following:

- Each infrastructure is modelled starting from the identification of components and their interactions;
- Each layer is defined with an appropriate level of abstraction based on information coming from end-users, stakeholders and open documents;
- Each component (we called it entity or agent) must be described in a way to decouple it from other components: the behaviour of the component must depend on the valued explicitly exchanged with the other components;
- The simulator must be able to represent any type of agent's behaviour for adapting to the specific reference scenario.

MHR approach allows to define three different typologies of agents: holistic agent, service agent and reductionist agents.

The infrastructure as a whole (or its general organizational divisions) is represented by a holistic agent (**Figure 2**) to provide a model that can understand the global interactions between infrastructures.

A service agent represents a logical or organizational aspect, that provides an aggregate resource as the remote control: the remote control generally provides supervision, by means of software and data collection. Data can be collected through telecommunication network or field equipment in case of a geographically distributed infrastructure. In **Figure 3**, a service component is depicted considering the classical model of an agent in CISIApro 2.0. Some examples of service are: the ability to supply customers, the ability to produce resources, the ability to

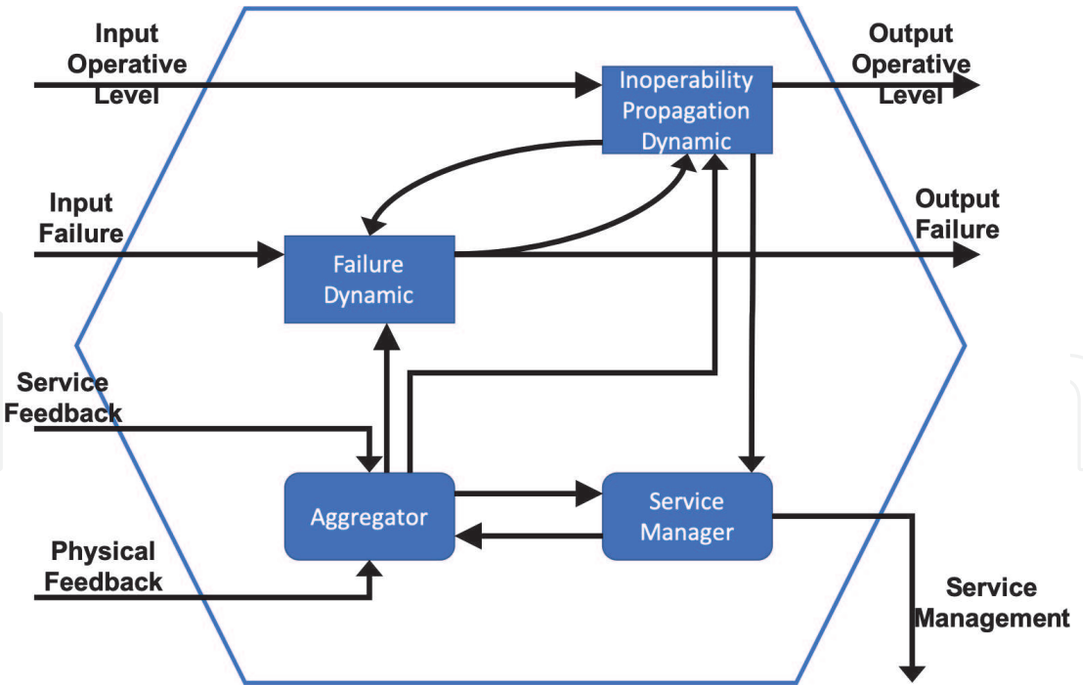


Figure 2.
The holistic agent representation.

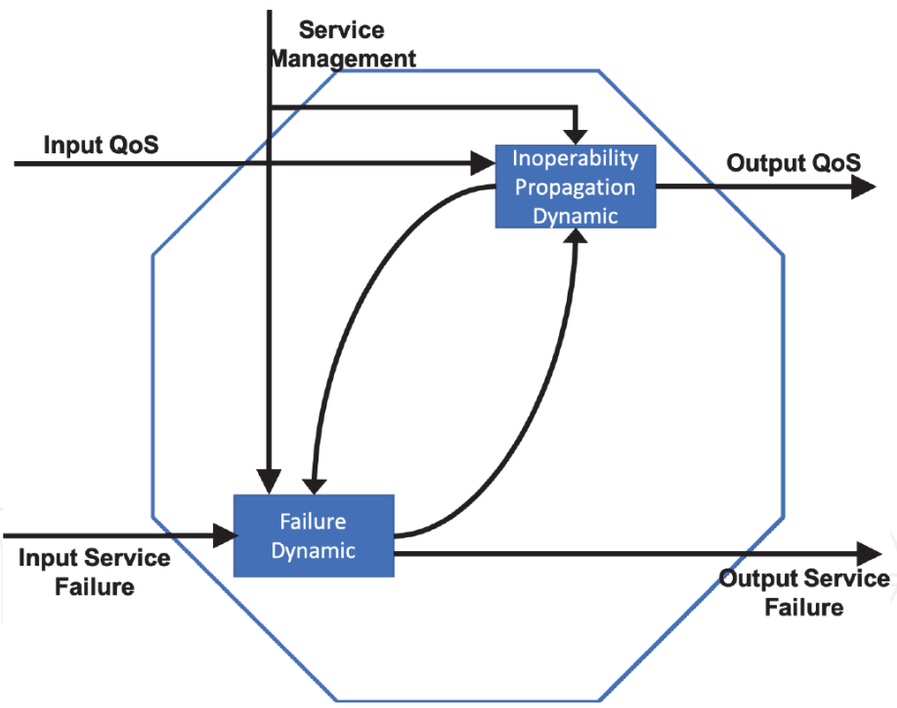


Figure 3.
The service agent representation.

change topology, the aggregate state of a subset of specific and important components.

Finally, with a reductionist agent, we can represent, with the right degree of abstraction, all physical or aggregated entities of the overall system. In **Figure 4**, the representation of a reductionist component is depicted. The picture does not explicitly consider a cyber threat: this malicious event can be represented in the same way as an input failure with a suitable "cyber dynamic".

Finally, we can represent, with the right degree of abstraction, physical or aggregated components of the overall system with a reductionist agent. The

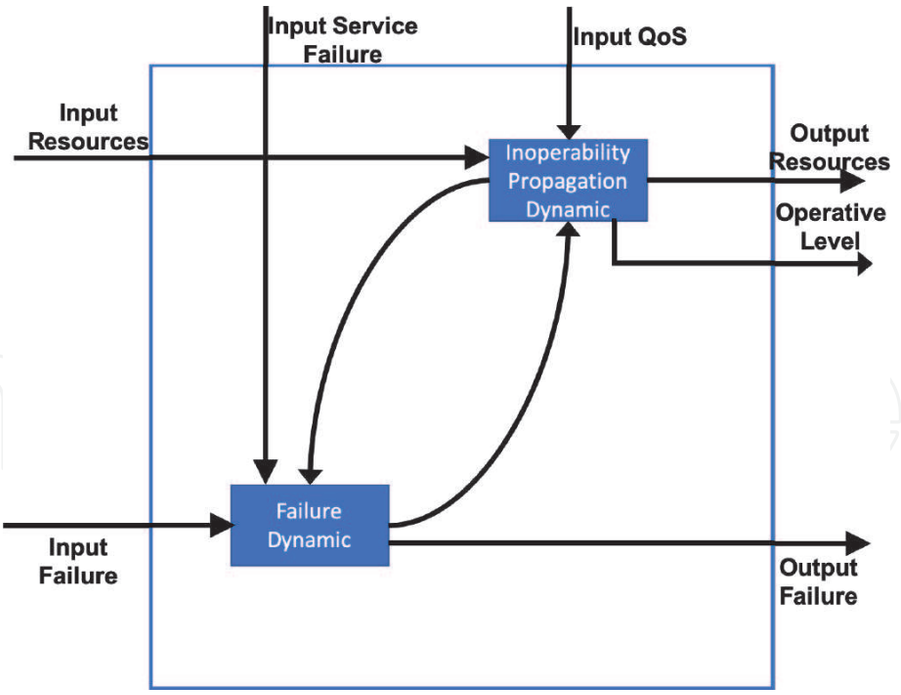


Figure 4.
The reductionist agent representation.

representation of a reductionist aspect is represented in the **Figure 4**. The input failure contains natural disaster events, failures and faults, but also cyber threats.

5. CISIApro 2.0 simulator

In this chapter, CISIApro 2.0 simulates the impact of anomalies and security attacks on the communication infrastructure and on the interlinked CIs. It will also support the decision-making process allowing a "what-if analysis" by simulating the application of countermeasures and reconfiguration and their impact on system resilience.

CISIApro 2.0 (Critical Infrastructure Simulation by Interdependent Agents) [11] is a software engine able to calculate complex cascading effects, taking into account (inter)dependencies and faults propagation among the involved complex systems.

CISIApro 2.0 is an Agent-Based simulation software consisting primarily of two modules, see **Figure 5**. The first one is the off-line tool in which it is possible to design and implement complex and highly interdependent scenarios. While the second one is the on-line tool which is implemented in Simulink (Mathworks).

CISIApro 2.0 is a database-centric architecture in which the database plays a key role as deonstrated in **Figure 5**. This implies a centralized asynchronous design that allows good modularity and scalability where each part of the IT infrastructure interacts, independently, with the centralized database in order to access the last data from the field (e.g. SCADA Systems), Complex Event Processing and generic IoT (Internet of Things) data systems, but also the simulation's outputs.

Using the Mixed-Holistic-Reductionist (MHR) approach, modelling complex interdependent systems is a prerequisite to produce an effective model. Once modelled the involved scenario, with MHR methodology can be applied with CISIApro 2.0.

From this point of view, CISIApro 2.0 engine does not only analyze actual situation and calculate the risk projected in the possible near future but, first, it

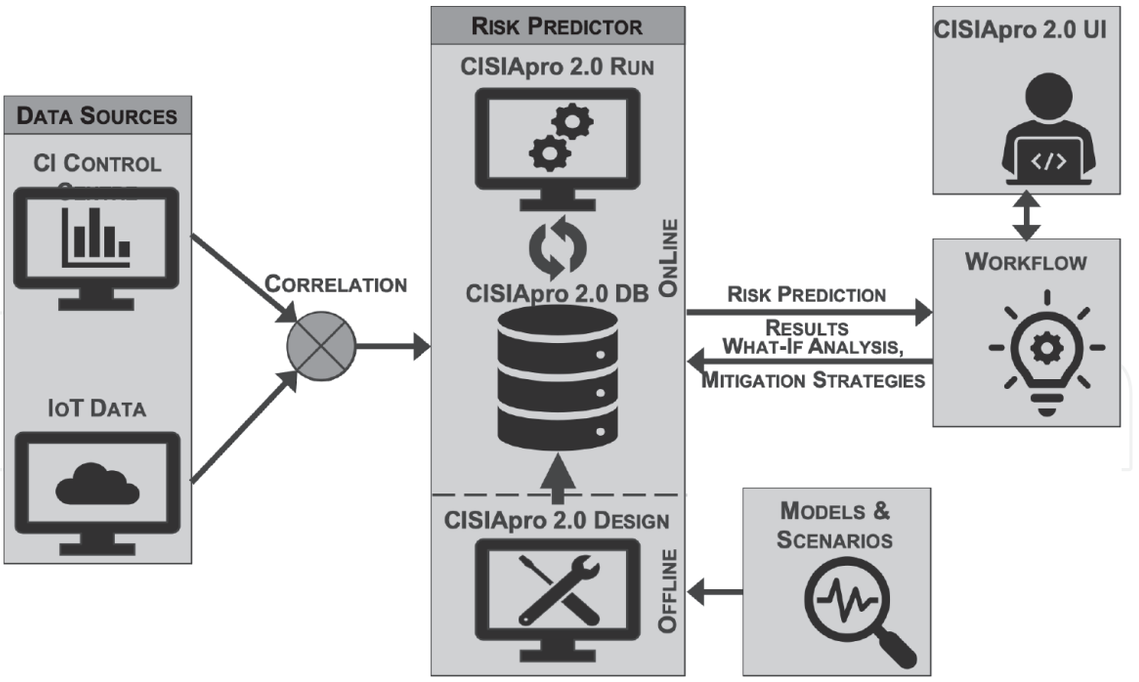


Figure 5.
CISIApro 2.0 architecture.



Figure 6.
CISIApro 2.0 Graphical User Interface.

plays the important role of Hybrid Risk Evaluation Tool. Hybrid because it is able to get information of different natures (sensor and data acquisition and complex event processing systems) and translating them in operational levels of resources, faults or services for the entities introduced in the critical infrastructure model.

With the proposed architecture, through CISIApro 2.0 modelling software, it is possible to dynamically change the interdependencies model and plugin other modules in order to have a pseudo-real-time scalable and flexible system, which can be changed at any time. The DB stores the information needed for the representation of several Critical Infrastructures, such as:

- Each entity is a specific instance of an entity type;
- Each entity has a status made of variables with values;
- Each entity has ports for exchanging resources;
- Each resource is associated with a MHR layer/net;
- Each layer has proper interdependencies;
- Each interconnection is made of a couple of ports, associated to two entities.

It should be noted that CISIApro 2.0 has introduced efficient ways to model, execute and debug simulations and cascading effects. In particular, an intuitive Graphical User Interface, **Figure 6**, is provided to create entities and connect them in easy way.

6. Case study and results

The proposed scenario consists of three major components: the telecommunication network, the hospital ward and the smart factory. For industrial automation and possible remote operations, the fifth generation of telecommunication networks would be an essential improvement [12].

The telecommunication network of the reference scenario is represented in **Figure 7**. The purpose of this network is to manufacture and deliver services and it has a hierarchical structure consisting of three main sectors: backbone, metro and access networks.

The Optical Packet Backbone (OPB) is a multi-service network that exchanges voice, data and video services. This network is based on IP/MPLS (Multi-Protocol Label Switching) technology and the network is fully redundant in all its components and resistant to failure conditions to ensure a high level of the delivered services.

The Optical Packet Metro (OPM) network is a metropolitan and regional collection and aggregation network capable, depending on the configuration, of managing traffic flows at the Ethernet, IP or MPLS level. Like OPB, the OPM network is a multi-service network in which both fixed and mobile services combine and, as such, guarantee the requirements of scalability, reliability, availability, and flexibility. The access network meets end-users in the telecommunications industry and greatly influences the features of the service offered.

There are several systems, each with varying efficiency and coverage zones, to build “the last mile”, which is the part of the network that stretches from the client site to the first access node. The latest generation of access network (GPON-Gigabit Passive Optical Network) based on fiber optic infrastructure with OLT (Optical Line Terminal) and ONU (Optical Network Unit) is briefly described at the bottom left of **Figure 7**.

The distinctive aspect of this technology is the development of a network in which many recipients are reached by a single optical fiber: this enables you to prohibit the introduction of individual fiber ties between the control panel and the receiver, thus minimizing the cost of infrastructure.

In the central part of the figure, we have a broadband network. The strength of this technology, which has encouraged its growth and proliferation, lies in the fact that voice and data services use the same copper cables as the conventional telephone network. Data traffic received by the consumer is isolated by a splitter from voice traffic and processed by a Digital Subscriber Line Access Multiplexer

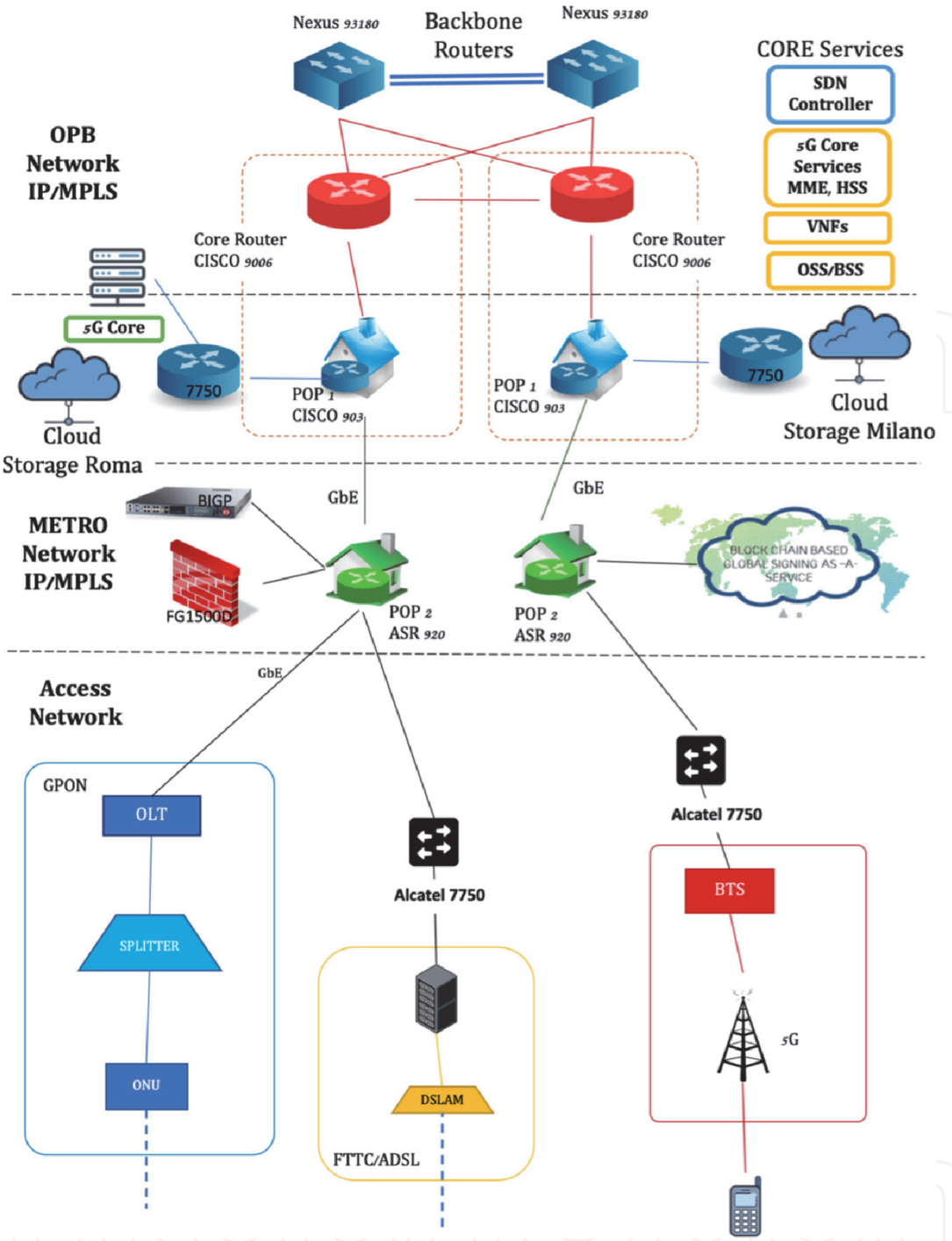


Figure 7.
The representation of the telecommunication network of the scenario.

(DSLAM) where the users' broadband lines connected to that particular central station are terminated.

On the right side of the picture, we insert the mobile network with the Base Transceiver Station (BTS) of the GSM networks that consist of antennas and transceivers responsible for the radio coverage of the territory.

The security fabric and data-center layer are achieved using a few next-generation security devices and application controllers as:

- Fortinet FortiGate (URL Filtering, Centralised Antivirus, Intrusion Detection and Protection System, E-mail filtering, Layer 4 Firewall)

- F5 BIGIP (Web Application Firewall).

Linked to the telecommunication network, we have a hospital ward represented in **Figure 8** that has been simplified to be modeled. This ward consists of a portion of the electrical grid in the yellow blocks, the water networks in blue blocks, the HVAC (Heating, Ventilation, and Air Conditioning) system in green blocks. We also add the building, made of eight rooms, where two are the operating rooms, and six are other rooms. These are the physicians' room, the staff room, the rooms used for visits, the surgery, and the waiting room, and the storage of medication and surgical supplies. These two types of rooms are modeled distinctly to underline their different relevance in the ward: while the medical and operating rooms are dedicated to patient care, must continue to provide the services requested optimally even after a failure, on the contrary, a malfunction of ordinary rooms does not drastically affect the quality of the service offered by the entire department.

The telecommunication network facilitates electrical hospital records to be processed in the clouds and relies on network-connected medical devices and systems.

Linked to the telecommunication network, a smart factor is present and is modeled in **Figure 9**. The smart factory for this scenario was modeled with reference to the radio access network architecture implemented in the factories of the future. **Figure 9** shows a completely autonomous local architecture, characterized by a pico site and an on-premises data center hub, which stores and performs data processing locally. The pico site is a small cellular base station typically covering a small area.

The 5G network is the best solution for this scenario [13, 14], which also makes it possible to incorporate the remote control of robots: according to this model, in a cloud environment, rather than in the robot itself, various functions aimed at regulating motion can be stored. It is thus assumed that the security of the networks in which the control modules work from cyber attacks is of vital importance.

The scenario contains also several services, modeled as service agents in CISIApro 2.0. Among those services, we focus our attention on the "5G Service", which is also included in **Figure 7**. 5G technology helps you to manage and control the movements of the programmable robotic arms remotely, increase human-machine interaction, capture the information processed by these intelligent systems and handle them in real-time. With regards to the hospital, the goal is to pervasively

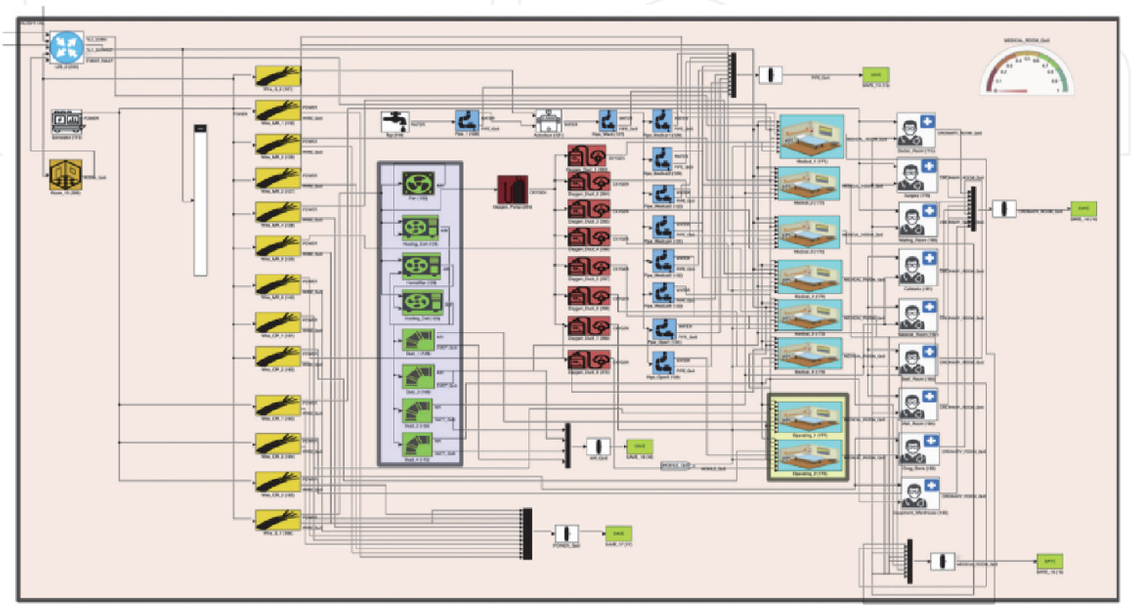


Figure 8.
The hospital in CISIApro 2.0 simulator.

DOI: http://dx.doi.org/10.5772/intechopen.94506

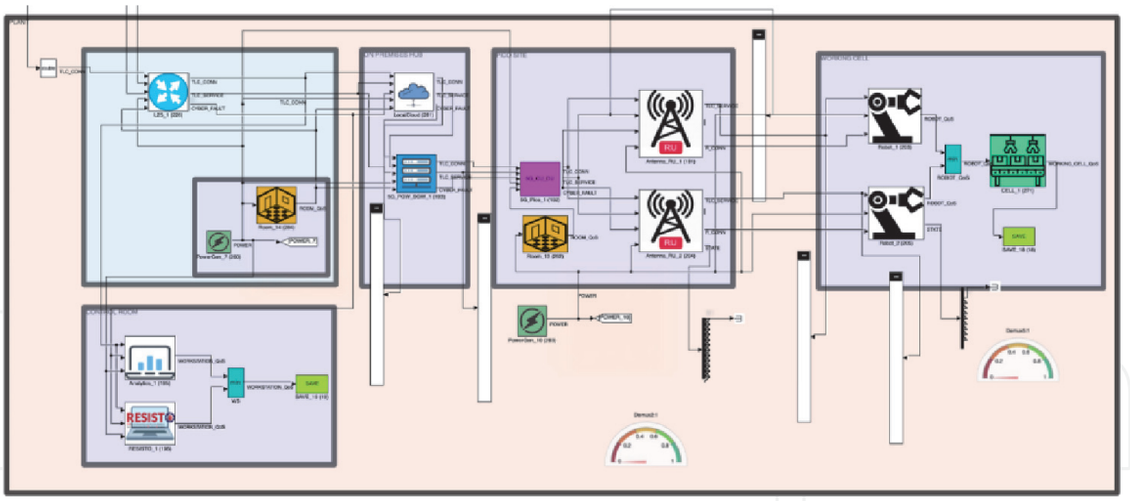


Figure 9.
The factory in CISIApro 2.0 simulator.

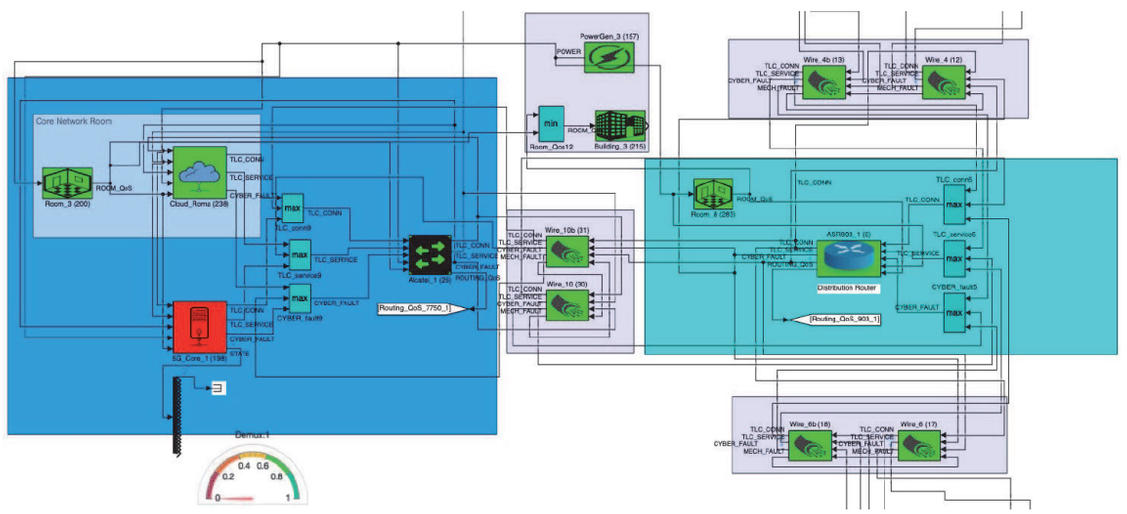


Figure 10.
The consequences on the "5G Core" component.

interconnect healthcare structures, doctors, patients, and healthcare personnel, to increase efficiency and effectiveness. In this context, the capabilities of 5G are useful for remote surgery, for remote control of the vital parameters of patients recovering from or suffering from chronic conditions and for exchanging medical data in real-time between the different technical figures.

The case study aims to examine the effects of a cyber-attack on the 5G core component, explicitly a DoS (Denial of Service). In this situation, we are not interested in how this attack was carried out, but we are more interested in the possible consequences of interconnected facilities.

The operative level of the "5G Core" agent is zero, as depicted in **Figure 10**, because it is the node that can not produce any output resource. The other entities of the telecommunications are not affected by this cyber-attack, because they don't need this service to properly work.

Different consequences affect the hospital and the smart factory. The domino effect on the smart factory is depicted in **Figure 11**. In the factory, there are four entities that need the 5G Core services to work: those entities are 5G-PGW-SGW, 5G-Pico, and the two antennas RU. Those elements are the red blocks in **Figure 11**, and they have an operative level equal to zero because they can not properly produce their outputs.

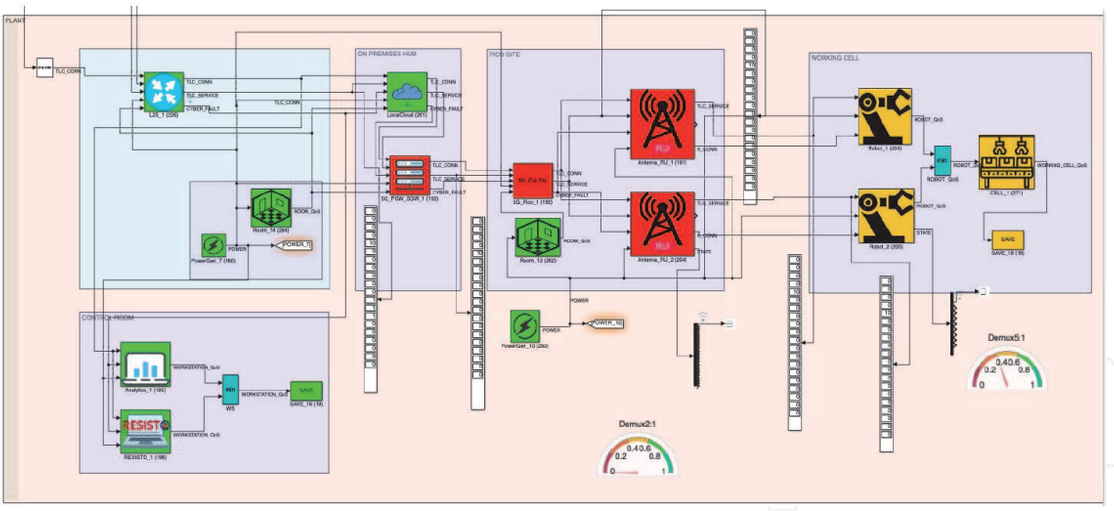


Figure 11.
The consequences on the factory section in CISIApro 2.0.

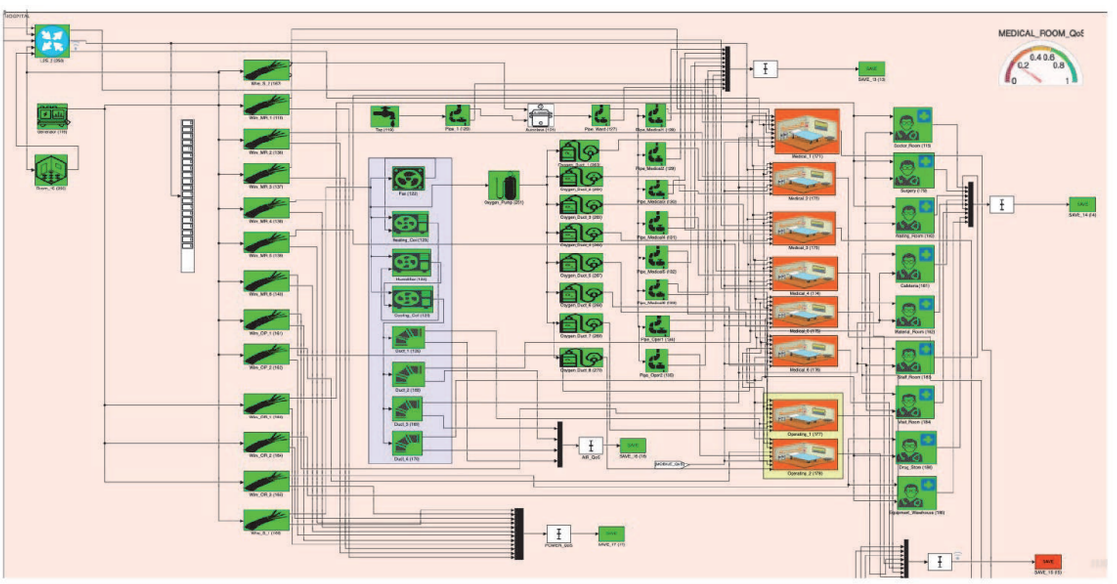


Figure 12.
The consequences on the hospital section.

Unlike the aforementioned elements, the two robots have an operative level of 0.4: although they cannot be controlled remotely or the information processed by them can be collected, however, these intelligent systems continue to operate.

In **Figure 12**, the output for the hospital is depicted. The absence of the 5G service has a more significant impact on medical rooms and operating rooms, due to the importance that hospital infrastructure has. In fact, despite following the cyber attack, it is no longer possible to carry out remote surgery, remotely monitor the vital parameters of patients and manage electronic medical records, these health rooms are still available for use and to ensure adequate care for patients.

7. Conclusions

This chapter analyses the concept of risk and resilience for critical infrastructures. The two concepts are tied together: minimizing risk means improving

resilience. In critical infrastructure protection world, assessing risk is very complex due to, among the others, due to interdependency: managing risk is well-established in each infrastructure, but the risk of interconnected infrastructures is still an open problem without a single solution.

Modelling infrastructures and their interdependencies could help in managing risk and also resilience. The proposed approach is called MHR and it is implemented with CISIApro 2.0, an agent-based simulator, which assesses the consequences of events on the reference scenario. We test the proposed approach into a telecommunication scenario, with a hospital ward and a smart factory. The results demonstrate the correctness of this approach that is currently under validation within the EU H2020 RESISTO project. During the project, the system will be integrated into real test-bed provided by various telecommunication providers.

Acknowledgements

This chapter is partially supported by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 786409 (RESISTO - RESIlience enhancement and risk control platform for communication infra-STructure Operators).

Conflict of interest

The authors declare no conflict of interest.

Author details

Chiara Foglietta*† and Stefano Panzieri†
University of Roma Tre, Rome, Italy

*Address all correspondence to: chiara.foglietta@uniroma3.it

† These authors contributed equally.

IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Department of Homeland Security (DHS). National Infrastructure Protection Plan: 2007/2008 Update. Technical report, 2007.

[2] European Parliament. Directive 2002/91/EC of the European Parliament and of the Council of 16 December 2002 on the energy performance of Buildings 2009.

[3] O'Rourke T, Briggs T. Critical infrastructure, interdependencies, and resilience. The Bridge. 2007;**37**:01

[4] Merriam-Webster. Resilience.

[5] Michel Bruneau and Andrei Reinhorn. Overview of the resilience concept. In *Proceedings of the 8th US national conference on earthquake engineering*, volume 2040, pages 18–22, 2006.

[6] DHS Risk Steering Committee et al. Dhs risk lexicon. *Department of Homeland Security Tech. Rep*, 2008.

[7] Kasthurirangan Gopalakrishnan and Srinivas Peeta. *Sustainable and resilient critical infrastructure systems: simulation, modeling, and intelligent engineering*. Springer, 2010.

[8] Steven M Rinaldi, James P Peerenboom, and Terrence K Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6):11–25, 2001.

[9] Haimes YY, Jiang P. Leontief-based model of risk in complex interconnected infrastructures. Journal of Infrastructure Systems. 2001;**7**(1):1-12

[10] Giusj Digioia, Chiara Foglietta, Stefano Panzieri, and Alessandro Falleni. Mixed holistic reductionistic approach for impact assessment of cyber attacks. In *2012 European Intelligence and Security Informatics Conference*, pages 123–130. IEEE, 2012.

[11] Chiara Foglietta, Cosimo Palazzo, Riccardo Santini, and Stefano Panzieri. Assessing cyber risk using the cisiapro simulator. In *International Conference on Critical Infrastructure Protection*, pages 315–331. Springer, 2015.

[12] Mansoor Shafi, Andreas F. Molisch, Peter J. Smith, Thomas Haustein, Peiying Zhu, Prasan De Silva, Fredrik Tufvesson, Anass Benjebbour, and Gerhard Wunder. 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. IEEE Journal on Selected Areas in Communications, 35(6):1201–1221, jun 2017.

[13] Sriganesh K Rao and Ramjee Prasad. Impact of 5g technologies on industry 4.0. *Wireless personal communications*, 100(1):145–159, 2018.

[14] Massimo Condoluci, Maria A Lema, Toktam Mahmoodi, and Mischa Dohler. 5g iot industry verticals and network requirements. In *Powering the Internet of Things With 5G Networks*, pages 148–175. IGI Global, 2018.