Modeling Telecommunications Infrastructures Using the CISIApro 2.0 Simulator

Elena Bernardini, Chiara Foglietta, Stefano Panzieri

Chapter 1

MODELING TELECOMMUNICATION INFRASTRUCTU BY CISIAPRO 2.0 SIMULATOR

Elena Bernardini, Chiara Foglietta and Stefano Panzieri

Abstract Telecommunications are an important part of our lives and they are a vital component of Industrial and Automation Control Systems (IACSs) that control Critical Infrastructures. Nowadays, the integration of IACS with the Information Technology system is a reality, mainly due to economic saves. However, this integration has lead to new troubles related to the spread of cyber threats which can be caused also damage to the physical infrastructures. Telecommunications are one of the possible reasons for which an adverse event on a single infrastructure can be amplified giving rise to high-impact crises.

Modeling Critical infrastructures is a complex and multi-disciplinary problem that is mandatory to understand the domino effect on interdependent complex networks. CISIApro 2.0, an agent-based simulator, models interconnected infrastructures to assess the consequences of adverse events, such as failures, cyber-attacks, and natural disasters, and restoring actions. CISIApro 2.0 has been adapted to model telecommunication infrastructure, in terms of network routing and the allocation of differentiated services. CISIApro 2.0 is validated in a modern telecommunication network within the European H2020 RESISTO project. RESISTO helps communication infrastructures operators during the decision process exploiting the combined use of preparatory analyses, detection and reaction technologies in the physical and cyber domains.

Keywords: Critical Infrastructures, Modeling, Agent-Based Simulator, Telecommunication, Cyber Attack

1. Introduction

New telecommunication infrastructure enables sparsely networks over extensive areas, offering excellent coverage and having an enormous effect on people's lives. In recent decades, the use of telecommunica-

tions and network reliability has risen exponentially, and our reliance on telecommunications has become the most critical factor in how people live during a crisis [27].

Telecommunications are changing, facing new challenges. The extensive amount of mobile data traffic led to the development of fifth-generation (5G) networks [3]. Another important challenge is the massive connectivity. The number of connected devices composes the Internet of Thing environment, which will support massive machine-to-machine communication.

Applying the IoT paradigm into Critical Infrastructure means supporting collaboration and connection between objects automatically [29]. Critical Infrastructures are controlled from remote through SCADA (Supervisory Control and Data Acquisition) systems. SCADA networks are changing due to the pervasive introduction of the Industrial Internet of Things causing a change also in architecture [5].

SCADA networks were based on the "air-gap" principle: they were usually disconnected from the Ethernet-based networks (i.e., Internet) and they exploited proprietary protocols. Now, they are moving to the Internet, exploiting the new capabilities that actual technology in communication can offer. This change improves the efficiency of the systems but it also causes an increment in the attack surface of cyber threats.

Assessing risk in critical infrastructure is a well-known problem. 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" [**?**]. Risk is thus traditionally defined 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 degradation of the asset. Risk management involves knowing the threats and hazards that could affect an asset, assessing the vulnerabilities of the asset and then evaluating the impacts on the asset. Based on these characteristics, it is possible to develop specific indicators and metrics to assess the risk to critical infrastructure.

Also, the concept of resilience [7], like the concept of critical infrastructure, is evolving: the resilience of an organization reflects the degree of preparedness and the ability to respond to and recover from a disaster or, in general, a negative event. Because lifeline systems are intimately linked to the economic well-being, security, and social fabric of a community, the initial strength and rapid recovery of lifelines are closely related to community resilience [6].

The concepts of risk and resilience are similar and they are tight connected: improving the resilience of the system means decreasing risk.

Risk is usually organized in terms of preparedness, mitigation measures, response capabilities, and recovery mechanisms; the traditional components of resilience are anticipation, absorption, adaptation, and recovery. Risk is usually related to a possible metric for understanding the consequences of adverse events; resilience is the ability to decreasing the effects of adverse events. In this paper, the two concepts are exploited for understanding the consequences of adverse events (such as natural disasters, cyber-attacks or faults) and the consequences of restoration or mitigation actions.

1.1 Contributions

The modeling approach exploited in this paper is based on the Mixed Holistic Reductionist (MHR) approach, where each infrastructure is divided into components (reductionist layer), services (service layer) and holistic nodes (holistic layer). This approach is then applied using an agent-based simulator, called CISIApro 2.0. This simulator can represent the consequences of adverse and positive events in an interdependent scenario. This simulator runs in real-time connected to a SCADA control center to acquire updated information on faults and connected to an Intrusion Detection System (IDS) to acquire actual threats and on-going cyber-attacks. CISIApro 2.0 can integrate heterogeneous data to improve the situational awareness of operators and their decision-making process. The reference scenario includes some elements that are envisioned in 5G technology.

1.2 Organization

The paper is organized as follows. Section1.2 reviews the literature on modeling activities for critical infrastructure interdependencies; in Section1.3, the Mixed Holistic-Reductionist (MHR) approach is presented, with Section1.4 presenting the agent-based simulator called CISIApro 2.0; the case study is detailed in Section1.5, in terms of components and results; Section1.6 includes the case study and the results are presented; and, finally, conclusions and future works are discussed in Section1.7.

2. Literature Review

In literature, critical infrastructure modeling has three main methodologies: agent-based simulation, input-output analysis, and network modeling. Heterogeneous and/or unclassified methods can be found in literature [15].

The agent-based simulations consider each infrastructure as complex adaptive systems, consisting of agents representing single facets in the infrastructure itself. Each agent may be represented at various degrees of abstraction, depending on the proposed resolution modeling stage. The principal advantage of agent-based simulation is the potential to establish synergistic strategies as agents begin to communicate with each other [23].

The second method is based on the economic theory of Input-Output pioneered by Leontief in the early 1930s but later applied to model infrastructures. To research the impact of interdependencies on the inoperability of interconnected networked systems, Haimes and Jiang developed the linear Input-Output Inoperability Model (IIM) [16]. We are looking, for example, at a two-system model. If a failure in subsystem 1 results in subsystem 2 being 80% inoperable, and subsystem 2 failure renders subsystem 1 inoperable to 20%, the impact of functional loss due to an external interference can be determined by solving the Leontief equations. The key benefit of the IIM and its modification lies in the efficiency and versatility of the proposed solution. Usually, IIM is limited to the interdependencies economic costs.

Researchers have been developing new ways of modeling interdependencies of infrastructure in recent years. The most promising solution is based upon the theory of graphs and networks. In this method, infrastructures are defined using abstract graphs consisting of nodes and arcs, standing for relations between components in the infrastructures. The main benefit is to take advantage of closed-form expressions and numerical simulations to characterize their topology, performance, and uncertainty.

Several works reviewed the proposed approaches for modeling interdependencies between critical infrastructures; the reader can refer to [12], [24] and [21] for further information on this topic.

Telecommunication infrastructure is a key sector in modeling complex systems, but it is also very complicated. In the critical infrastructure protection field, researchers are usually focused on SCADA control network, as done in [9,13,14,18]. SCADA systems are computer-controlled devices that execute and transmit the physical changes in infrastructure networks to operators. SCADA network is a subset of a telecommunication network with specific protocols, such as DNP3.0 (Distributed Network Protocol), [28], or Modbus TCP/IP, [11].

Modeling telecommunication networks is usually realized with domain simulator such as NS3 [22] or queue models [2]. For instance, NS3 can analyze the consequences of perturbations to the normal operation of the network [8].

In this paper, we approach the problem of modeling telecommunication networks as part of an even more complex scenario made of other infrastructures, such as hospitals and smart factories. In the next section, we describe the proposed approach for modeling interdependent infrastructures.

3. Modeling Interdependencies with MHR approach

We present a method for support during the modeling process in this paper. The Mixed Holistic Reductionist (MHR) [10] methodology exploits the advantages of both methods: holistic and reductionist. The key goal of the MHR methodology is to provide a potential guideline for careful model critical infrastructures and their interdependencies.

In holistic modeling, infrastructures are seen as individual entities with well-defined borders and functional property, creating a global and overall overview. Viewing an infrastructure as a single entity means to define and describe the different infrastructures and their regional extent. The volume of data needed for modeling activities is very small at this level and can be found in public datasets.

The reductionist paradigm, on the other hand, stresses the need to better consider the functions and actions of the individual components to properly appreciate the overall system. The reductionist method drills down to each part in terms of inputs and outputs. Throughout this level of abstraction, relations between the machinery and single elements can be readily established.

Different systems require various degrees of analysis and their limits are lost in the event of complex case studies. In the MHR model, network relationships may be seen at various levels, either from a top-down or bottom-up strategy. The other main benefit is to model infrastructures at a different level of abstraction level, given the amount of available data.

The connection point between the two layers of complexity, i.e. holistic and reductionist approaches, is the assessment of service efficiency (hereinafter abbreviated as "service"), which is a critical aspect for operators. This layer explains the functional relationships at various rates or granularity between components and infrastructures. MHR specifically identifies services to customers and other linked infrastructures to be a middle layer between holistic and reductionist levels.

Through limited data and gathered information, the MHR helps to achieve the correct level of detail. In the following, some essential considerations can be summarised:

- Each network is modeled starting with component recognition and their interactions;
- An effective level of abstraction is established for layer based on inputs from end-users, stakeholders and open documentation;
- Every component (which we call entity or agent) must be defined in such a way as to decouple it from other components: the component's behavior must depend on the valued directly shared with the other components;
- The simulator, which applies the MHR approach, must be able to represent the behavior of any sort of agent for adaptation to the particular reference scenario.

The MHR approach allows for three different categories of entities to be defined: holistic entities; service entities and reductionist entities.

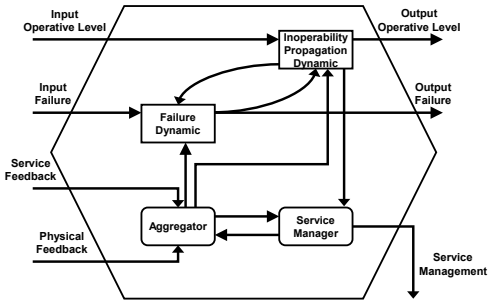
A Holistic Entity (Figure1a) represents the infrastructure as a whole (or its general functional divisions) to provide a paradigm that might potentially understand the global interactions within the infrastructure to reflect actions relevant to policies, strategies, etc.

A Service Entity is a functional or operational function that offers an integrated resource as a remote control: remote control typically refers to a supervisory mechanism by software and data collection. In the case of a geographically dispersed system, data can be obtained via telecommunication network or field equipment. A service component in CISIApro 2.0 is depicted in Figure1b, representing the classical concept of an agent in CISIApro 2.0. Such examples of service are:

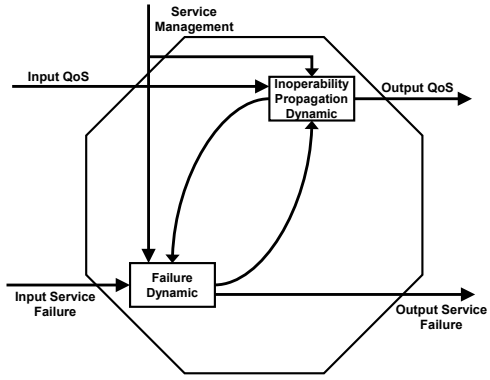
- the ability to serve customers
- the ability to produce resources
- the ability to adjust topology
- the status of other unique and essential components.

Finally, for a Reductionist Entity, we can describe all actual or aggregated aspects of the total system, with the right abstraction degree. The representation of a reductionist component is depicted in Figure1c. The picture does not specifically identify a cyber threat: this malicious event may be interpreted in the same manner as an input failure with an acceptable "cyber dynamic".

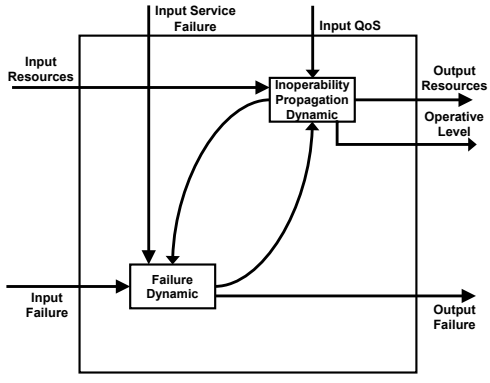
The MHR approach helps the developer to depict a specific scenario into various functional components. The layers allow the modeling a



(a) Holistic entity representation



(b) Service entity representation



(c) Reductionist entity representation

Figure 1: MHR representation of different entities at different abstraction layers

complex situation, consisting of many interconnected infrastructures, of various degrees of abstraction: an infrastructure can be modeled in all its features (reductionist, service and holistic layers), another can be modeled using just the holistic layer, without any problem aside from the granularity and the precision of the results.

4. Dynamic Risk Propagation using CISIApro 2.0

CISIApro 2.0 (Critical Infrastructure Simulation by Interdependent Agents) [14, 19] is a software engine capable of measuring complex cascading effects, taking into account (inter)dependencies and fault propagation among the complex systems concerned. CISIApro 2.0 may also suggest prevention and restoration steps determining their positive effects. Under the H2020 ATENA project [1] CISIApro has built from scratch in 2011 to enhance the modeling process of the interdependencies between infrastructures. CISIApro has been updated to version 2.0 during the H2020 RESISTO project [4], incorporating several significant functionalities related to the simulation of telecommunications infrastructures.

CISIApro 2.0 is an agent-based simulator, with each agent having the same structure. In particular, each agent receives resources and faults from the upstream agents and distributes them to the downstream ones, as seen in Figure2. The layers are derived from resource or fault propagation. A resource is a commodity or a data generated and/or consumed by the agent which is defined as an entity in CISIApro 2.0. The entity often produces or receives failures (generally, malfunctions) which reflect a physical failure or a possible cyber attack. The malfunctions are distributed among the agents following various propagation models which take into account the interdependency class (i.e., layers) and information reliability. The layers under consideration are physical, logical, geographical and cyber.

The capacity to generate resources is defined by the idea of the operational level, based on the availability of resources provided, the proliferation of faults, and the entity's functionality.

Each agent's operational level can be considered as a risk metric. The risk is typically a numerical measure, from the magnitude of the effect, the probability of incident or threat, and the measurement of the vulnerability. In CISIApro 2.0 implementations, the probability of an event is generally considered more related to the definition of the information's trustworthiness. The user may also add a vulnerability variable for each entity, but we presume that the vulnerability depends

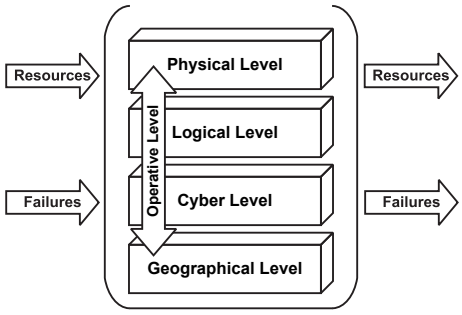


Figure 2: CISIApro 2.0 entity representation

only on the distance from the source and on the duration of the attack itself. The agent's operational level is correlated with a risk rating: the risk is the amount of harm due to specific incidents, such as a cyber attack, and can be measured as

$$Risk = 1 - OperationalLevel \tag{1}$$

where 1 is the maximum value of the operational level. A higher operational level value means a lower risk. Operational level, therefore, reflects a complex risk evaluation which takes into account the cascading consequences of adverse events, i.e., natural disasters, failures or cyber-attacks. For each infrastructure, this value is standardized considering the quality of service towards customers and other infrastructures.

4.1 CISIApro 2.0 Implementation Details

CISIApro 2.0 consists primarily of two units, as seen in Figure 3. The first one is the off-line tool known as "CISIApro 2.0 Design", which enables dynamic and highly interdependent scenarios to be planned and implemented. While the second is the CISIAmat (or "CISIApro 2.0 Run") online tool that exploits Simulink Mathworks for the real-time engine that is currently linked to near real-time data sources.

CISIApro 2.0 is a software platform built on a database-centered architecture where the database plays a central role, called in Figure3 "CISIApro 2.0 DB". This means a distributed design that allows for horizontal scalability where every element of the architecture for risk propagation independently interacts with the centralized database to collect the last data from the field and the output of CISIApro 2.0.

"CISIApro 2.0 Run" engine generates an impact estimation of any observed abnormalities. The decision maker, often assisted by a workflow manager, should select from various sequences of potential reaction techniques to minimize the results, often taking into account CISIApro

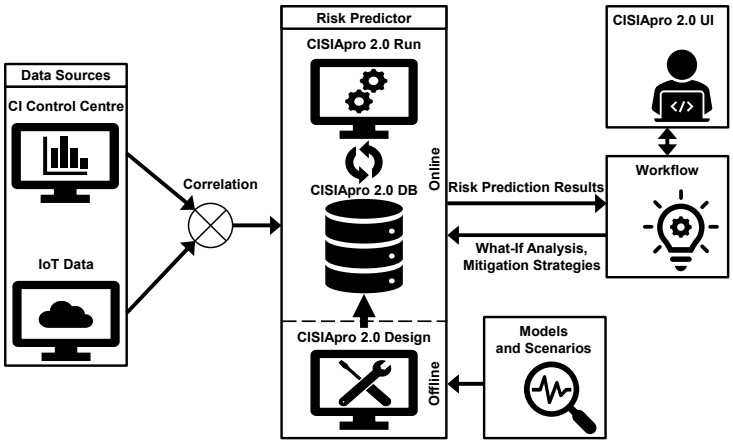


Figure 3: CISIApro architecture

Figure 4: Graphical User Interface of CISIApro 2.0 Design

2.0 output. CISIApro 2.0, starting from the real scenario and the level of QoS (Quality of Service) of systems concerned, simulates What-If scenarios to provide the decision maker with practical knowledge about future sensitive circumstances.

4.2 CISIApro 2.0 Mathematical Structure

In this section, we mathematically define the structure of the CISIApro 2.0, using a multilayer network.

We can formally define a graph (i.e., a single-layer network) as a tuple $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes and $\mathcal{E} = \mathcal{V} \times \mathcal{V}$ is the set of edges that connect pairs of nodes. Two nodes are called adjacent, if there exists an edge between them.

To model the Critical Infrastructure structure, in addition to classical nodes and edges entities, we need to expand the system's graph definition, with the concept of *layers*. Using the formalism of the multilayer networks [17], a complex system with d different types of layers is usually indicated as $\mathbf{L} = \{\mathcal{L}_a\}_{a=1}^{d}$, where other variables can be used to indicate whether a node is present in the considered layer.

We firstly construct a set $\mathcal{V} \times \mathcal{L}_1 \times \cdots \times \mathcal{L}_d$ and then define a subset $\mathcal{V}_M \subseteq \mathcal{V} \times \mathcal{L}_1 \times \cdots \times \mathcal{L}_d$ containing only the corresponding node-layer combinations. Let u and α_i be the considered node and layer respectively, then $(u, \boldsymbol{\alpha}) \equiv (u, \alpha_1, \ldots, \alpha_d)$ represents the set containing the topological connection (u, α_i) between node u on the layer α_i.

We can now introduce the edge set $\mathcal{E}_M \subseteq \mathcal{V}_M \times \mathcal{V}_M$, defined as the set of all possible combinations of node-layers. It should be noticed that different connection can be considered through this set, such as self node connection in different layers as well as multiple layer linking.

Finally, we can define a *multilayer network* as a quadruplet

$$M = (\mathcal{V}_M, \mathcal{E}_M, \mathcal{V}, \mathbf{L}). \tag{2}$$

Note that a single-layer network is a special case of a multilayer network, in which $d = 0$ and $\mathcal{V}_M = \mathcal{V}$ are redundant. Furthermore, given a subset $D \subseteq \mathbf{L}$ of the layers of the *multilayer network* M, a special set of nodes that can be reached by any edge starting from a generic node v from any of the layers in D, is called *neighborhood* and is formally defined as $\Gamma(v, D)$.

In what follows, the multilayer network structure of CISIApro 2.0 is addressed and the modelling for the interdependence risk assessment added.

In general, the first two elements in a multilayer network M generate a graph $\mathcal{G}_M(\mathcal{V}_M, \mathcal{E}_M)$, so we can view a multilayer network as a graph

whose nodes and edges are labeled in some way. We can easily say that a multilayer network M is directed if all the underlying graph $\mathcal{G}_M$ are directed. Mathematically, the $\mathcal{E}_M$ is an ordered set of edges, and therefore $((u, \boldsymbol{\alpha}), (v, \boldsymbol{\beta})) \neq ((v, \boldsymbol{\beta}), (u, \boldsymbol{\alpha}))$.

CISIApro 2.0 structure is a directed multilayer network where each agent is a node that exists in at least one layer but can also be included in all the layers. CISIApro 2.0 also uses the convention to disallow multilayer network self-edges by avoiding self-edges in the underlying graph, i.e., $((u, \boldsymbol{\alpha}), (u, \boldsymbol{\alpha})) \notin \mathcal{E}_M$.

CISIApro 2.0 structure connects each agent with the set of nodes identified by the same entity in different layers. Therefore, the coupling edges inside CISIApro 2.0 structure, denoted by

$$\mathcal{E}_C = \{((u, \boldsymbol{\alpha}), (v, \boldsymbol{\beta})) \in E_M | u = v, \forall u, v \in \mathcal{E}_M, \forall \boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbf{L}\} \tag{3}$$

are always present.

CISIApro 2.0 structure describes a layer through a propagation, diffusion or consensus model among the nodes in the considered layer. In Fig.5, a potential image of a multilayer graph is depicted. The multilayer network consists of three layers, where the coupling edges are the black dotted lines, the red dotted lines are inter-layer edges

$$\mathcal{E}_{inter} = \{((u, \boldsymbol{\alpha}), (v, \boldsymbol{\beta})) \in E_M | u \neq v, \boldsymbol{\alpha} \neq \boldsymbol{\beta}\} \tag{4}$$

and the other lines are the intra-layer edges

$$\mathcal{E}_{intra} = \{((u, \boldsymbol{\alpha}), (v, \boldsymbol{\beta})) \in E_M | u \neq v, \boldsymbol{\alpha} = \boldsymbol{\beta}\} \tag{5}$$

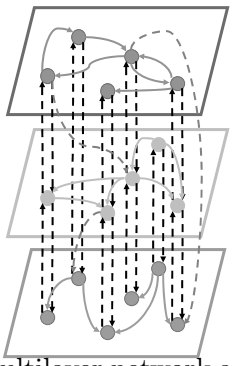


Figure 5: An example of multilayer network as in CISIApro 2.0 simulator

Each node $(u, \boldsymbol{\alpha})$ that occurs in at least one layer of M has a status vector $x_u(t)$ associated to define the evolution of the u component at time t. The status vector of each component is modeled as being governed by

a non-linear discrete dynamical equation, where the status changes for each u is modulated using its internal state $x_i(t)$ and the neighboring data obtained.

Formally, the discrete-time nonlinear dynamics of the status vectors at time k are specified as follows:

$$\begin{aligned} x_u(t+1) &= g_u\left(x_u(t), y_{\Gamma^+(u,\mathbf{L})}(t), z_u(t)\right) \\ y_u(t) &= h_u(x_u(t), z_u(t)) \end{aligned} \tag{6}$$

where g_u and h_u are nonlinear functions, $z_u(t)$ represents the external input for the node u and $y_{\Gamma^+(u,\mathbf{L})}(t)$ the received data from the incoming neighborhood. The incoming neighborhood of the node u is defined as:

$$\Gamma^+(u,\mathbf{L}) = \{v \in \mathcal{V}_M | ((v,\boldsymbol{\beta}),(u,\boldsymbol{\alpha})) \in \mathcal{E}_M, \boldsymbol{\alpha},\boldsymbol{\beta} \in \mathbf{L}\} \tag{7}$$

Without loss of generality, we can stack both the status vectors x_{ui} in a *state vector* $\mathbf{x}(t) = [x_1(t) \dots x_u(t)]^T, \forall u \in \mathcal{V}_M$, and the inputs into an *input vector* $\mathbf{z}(t) = [z_1(t) \dots z_u(t)]^T, \forall u \in \mathcal{V}$. Hence, the resulting dynamical system can be rewritten as:

$$\begin{aligned} \mathbf{x}(t+1) &= \mathbf{g}\left(x(t), \mathbf{y}_{\Gamma^+(\cdot,\mathbf{L})}(t), \mathbf{z}(t)\right) \\ \mathbf{y}(t) &= \mathbf{h}(\mathbf{x}(t), \mathbf{z}(t)) \end{aligned} \tag{8}$$

where $\mathbf{g}, \mathbf{h}$ represent the column vectors of $g_u, \forall u \in \mathcal{V}$ and $h_u, \forall u \in \mathcal{V}$, respectively.

As pointed out in [17], the dynamical model defined in (8) is general enough to include all the classical approaches already defined in Multi-layer Networks literature, such as percolation cascades or Susceptible-Infected-Recovered (SIR) models.

4.3 CISIApro 2.0 Dynamics

In the next section we describe the dynamics of CISIApro 2.0 using a max-consensus approach. For simplicity, we consider a layer of the multi-layer graph, generated by the propagation of a specific resource. The extension of the max-consensus approach to a multi-layer graph is straightforward.

We consider a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. For replicating the propagation algorithm implied in CISIApro 2.0, we partition the set of nodes into three subsets: the source nodes $\mathcal{V}_f \subset \mathcal{V}$, the sink nodes $\mathcal{V}_t \subset \mathcal{V}$ and the transmitting node $\mathcal{V}_m \subset \mathcal{V}$. Each node belongs to only one of this subsets and $\mathcal{V}_f \cup \mathcal{V}_m \cup \mathcal{V}_t = \mathcal{V}$. For each resource, there are some nodes generating this information (i.e., $\mathcal{V}_f$), some nodes receiving this information (i.e., $\mathcal{V}_t$) and the remaining nodes are just re-sent the information received.

The propagation algorithm in the simulator is based on some rules:

1 Each source node $i \in \mathcal{V}_f$ generates the resource (or a specific information), corresponding to its state (i.e., operating level) x_i, e propagates it to the successor nodes in broadcast manner. Notice that the information transmitted by each source node is orthogonal, or better distinguishable, from the messages propagated by the other source nodes;

2 The propagation of information from each source node to the destination node takes place through the transmitting nodes, with the following method:

$$x_i(k+1) = \max_{j \in \mathcal{J}_i} \{x_j(k)\}, \qquad i = 1, \ldots, n \tag{9}$$

where $\mathcal{J}_i$ is the set of predecessors of the node i and k is the communication event k-th;

3 Each sink node must receive at least one resource from one of the source nodes;

4 The sink nodes do not re-transmit any of the information received;

5 A fault in a transmitter node means that all its successors no longer receive the information that has been propagated up to that moment;

The *propagation algorithm* is defined if the destination nodes receive the information transmitted by the source nodes, i.e.:

$$x_i(k) = \max_{j} \{x_j(0)\}, \qquad i \in \mathcal{V}_t, j \in \mathcal{V}_f \tag{10}$$

The main concept is that the sink node needs the information transmitted by at least one source node: if there are two nodes transmitting a resource, the receiver needs the resource and usually don't care from which of the two nodes. The propagation algorithm is a specific case of the max-consensus algorithm, where we explicitly define the destination nodes.

Assuming that the topology of the communication network is fixed and that communication between the nodes takes place synchronously, that is, each node exchanges information with its neighbors simultaneously, *the maximum consensus algorithm* [20] is defined as follows:

$$x_i(k+1) = \max_{j \in \mathcal{J}_i} \{x_j(k)\}, \qquad i = 1, \ldots, n \tag{11}$$

where $\mathcal{J}_i$ is the set of predecessor nodes of node i and k is the communication event. We assume that $i \in \mathcal{J}_i, \forall i \in \mathcal{V}_f$, i.e., there exists a self loop only for source nodes.

Under these conditions, given an oriented graph $\mathcal{G}$ and the vector of the initial information states $x(0) := (x_1(0), ...x_i(0), ..., x_n(0))^T$, we can assure that *maximum consensus* is reached if $\exists l \in \mathbb{N}_0$ such that:

$$x_i(k) = x_k(k) = \max\{x_1(0), ..., x_n(0)\}, \forall k \geq l, \forall i, j \in \mathcal{V} \tag{12}$$

5. A Telecommunication Scenario

The proposed scenario is made of three main parts: the telecommunication network, the ward of an hospital and the smart factory. 5G telecommunication network will be an important change for industrial automation and possible remote surgery [25].

In Fig.6, the telecommunication network of the reference scenario is depicted. This network aims to produce and supply 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 platform where voice, data and video services travel. This network is based on IP/MPLS (Multi-Protocol Label Switching) technology and to ensure a high quality of the services provided, the network is completely redundant in all its components and immune to failure conditions.

The Optical Packet Metro (OPM) network is the metropolitan and regional collection and aggregation network capable of handling traffic flows at the Ethernet, IP or MPLS level depending on the configuration made. The OPM network, just like OPB, is a multi-service network in which all fixed and mobile services converge and as such must guarantee the requirements of scalability, reliability, availability, and flexibility. In telecommunications, the access network reaches end-users and determines significantly the characteristics of the service provided. To create "the last mile", that is the portion of the network that extends from the customer site to the first access node, there are multiple technologies, each having different performance and coverage areas.

In the bottom left side of Fig.6, is briefly depicted the new generation of the access network (GPON - Gigabit Passive Optical Network) based on fiber optic technology with OLT (Optical Line Terminal) and ONU (Optical Network Unit). The distinctive feature of this technology is the creation of an architecture in which a single optical fiber is used to reach multiple recipients: this allows you to avoid the deployment of individual fiber connections between the control panel and the recipient, thus reducing infrastructure costs. In the central part of the figure, we

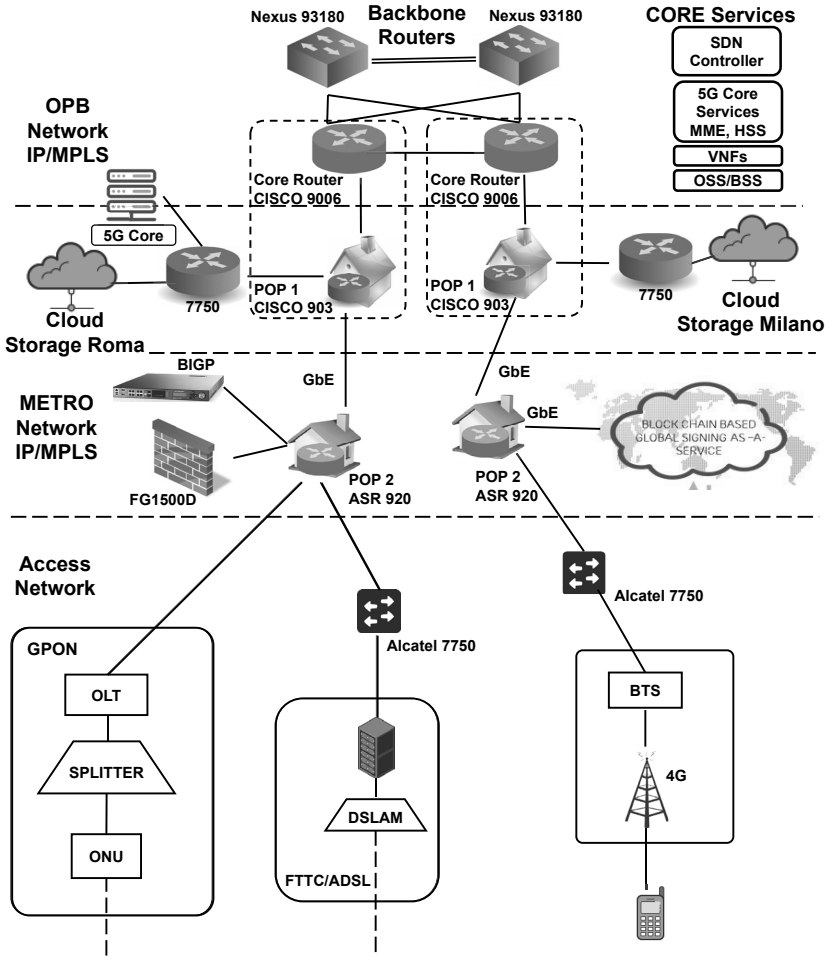


Figure 6: The representation of the telecommunication network of the scenario

have a broadband network. The strength of this technology, which has allowed its success and diffusion, lies in the fact that the same copper cables of the traditional telephone network are shared by voice and data services. The data traffic sent by the user is separated from voice traffic through a splitter and collected by the Digital Subscriber Line Access Multiplexer (DSLAM), where the broadband lines of the users assigned to that specific central station terminate. 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).

Connected to the telecommunication network, we have a hospital ward that has been simplified to be modeled represented in Fig.7. This ward is made of a part 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. Those are the doctors' room, the staff room, the rooms used for visits, the surgery, and the waiting room, and the storage of medicines and medical materials. 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 allows to store electrical hospital records in the clouds and to depend on medical devices and systems connected to the network.

Linked to the telecommunication network, a smart factor is present and is modeled in Fig.8. The smart factory for this scenario was modeled with reference to the radio access network architecture implemented in the factories of the future. Figure8 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 5G network then presents itself as the best solution for this scenario, which even allows the virtual control of robots to be implemented:

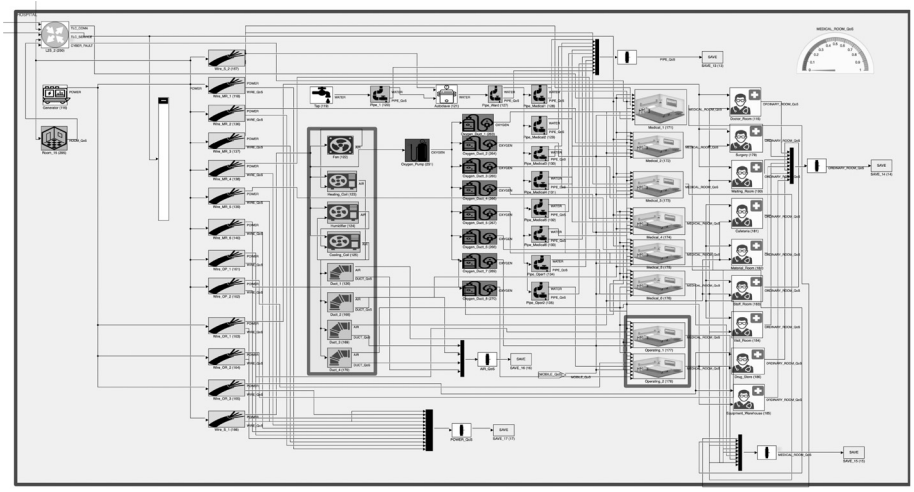


Figure 7: The hospital in CISIApro 2.0 simulator

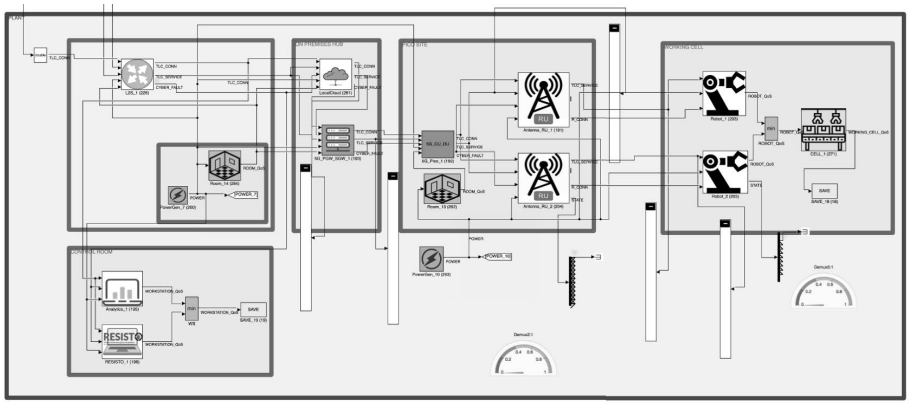


Figure 8: The factory in CISIApro 2.0 simulator.

according to this paradigm, various functions aimed at controlling motion can be located in a cloud system, rather than in the robot itself. It is therefore deduced that the protection against cyber attacks of the systems in which the control modules reside becomes of fundamental importance.

6. Case Study and Results

The scenario contains also several services, modeled as service entities in CISIApro 2.0. Among those services, we focus our attention on the "5G Service", also present in Fig.6. 5G technology allows you to re-

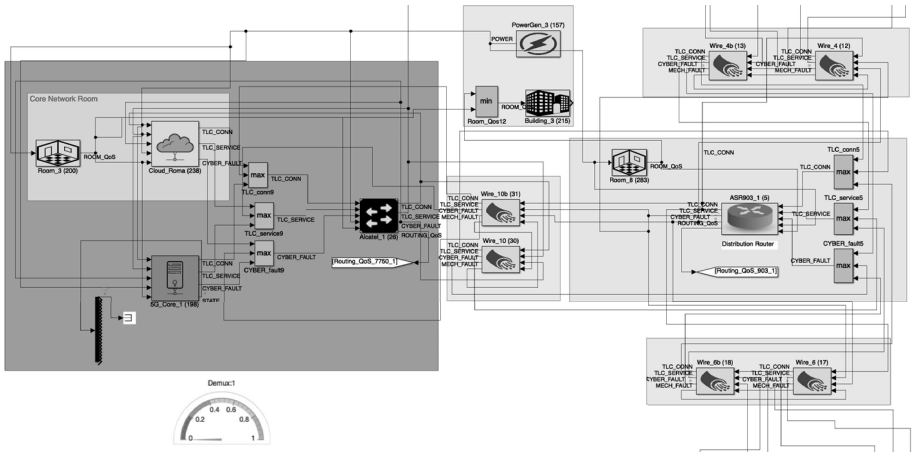


Figure 9: The consequences on the "5G Core" component.

motely manage and control the movements of the programmable robotic arms, improve human-machine interaction, collect the information processed by these intelligent systems and manage them in real-time. With reference to the hospital, the goal is to pervasively interconnect healthcare structures, doctors, patients, and healthcare personnel, in order to increase efficiency and effectiveness. In this context, the characteristics of 5G are useful for remote surgery, for remote monitoring of the vital parameters of patients recovering from or suffering from chronic diseases and for real-time communication of patient data between the various professional figures.

The case study wants to evaluate the consequences of a cyber-attack, specifically a DoS (Denial of Service), to the 5G core component. In this case, we are not interested in how this attack has been performed, but we are more interesting in the possible consequences of interconnected facilities.

The "5G Core" entity is zero, meaning that its operative level is zero, as depicted in Fig.9, 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 Fig.10. 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 Fig.10, and they have an operative level equal to zero because they can not properly produce their outputs.

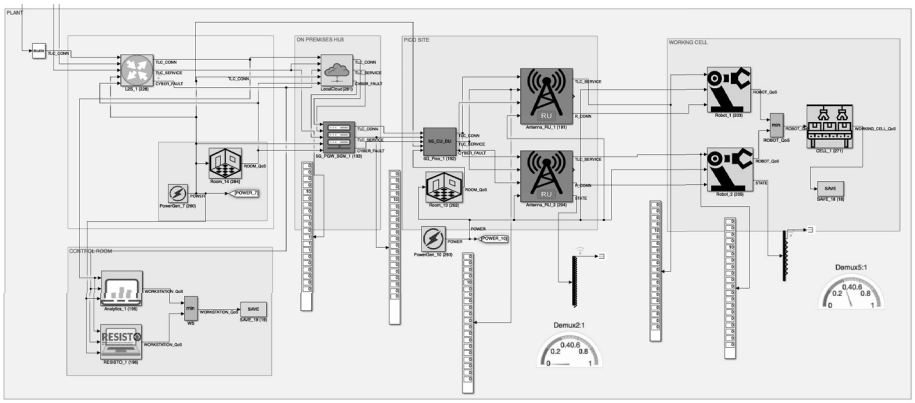


Figure 10: The consequences on the factory section in CISIApro 2.0.

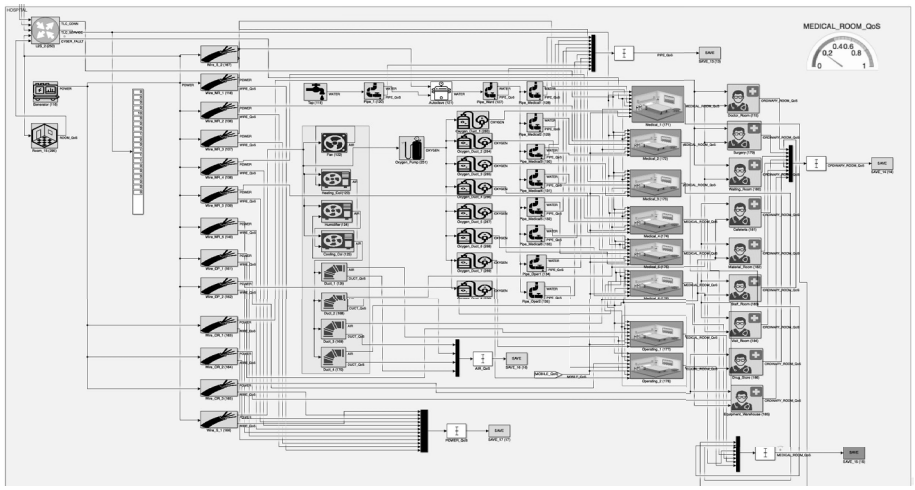


Figure 11: The consequences on the hospital section.

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 Fig.11, 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 and Future Works

The objective of this paper is to describe the complexity of telecommunication networks. Modeling is a challenge that is faced in the field of critical infrastructure protection, considering also the increasing number of possible cyber attacks against them.

This problem can be solved using CISIApro 2.0. This simulator has been re-designed and improved during 2019 to handle telecommunication network modeling. This paper describes CISIApro 2.0 simulator: CISIApro 2.0 is an agent-based simulator aiming at assessing the consequences of adverse events in an interdependent scenario. CISIApro 2.0 has two distinct phases: the first is the modeling activities and the second is the real-time simulator that evaluates the consequences of the adverse events connected to heterogeneous data sources. The output of CISIApro 2.0 is exploited in the decision-making process, to improve the operator situation awareness and to make better decisions knowing which are the consequences of actual events.

The case study demonstrates the ability of CISIApro 2.0 to handle a telecommunication network model and to assess the consequences of a cyber-attack in the connected infrastructures, such as hospitals and factories.

The work has been enlarged to consider different fault, different cyber-attacks and also different case studies, in the telecommunication field.

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 infraSTructure Operators).

References

[1] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. Di Giorgio, C. Foglietta, A. Galli, A. Giuseppi, F. Liberati, A. Neri, S. Panzieri, F. Pasucci, J. Proenca, P. Pucci, L. Rosa and R. Soua, Integrated protection of industrial control systems from cyber-attacks: the ATENA approach, *International Journal of Critical Infrastructure Protection*, vol. 21, pp. 72–82, 2018.

[2] A. S. Alfa, *Queueing Theory for Telecommunications: Discrete Time Modelling of a Single Node System*, Springer Science+Business Media, Berlin, Germany, 2010.

[3] N. Al-Falahy and O. Alani, Technologies for 5G networks: Challenges and opportunities, *IT Professional*, vol. 19(1), pp. 12–20, 2017.

[4] E. Aonzo and A. Neri, RESISTO: Resilience Enhancement and Risk Control Platform for Communication Infrastructure Operators, Leonardo - Cyber Security Division, Rome, Italy, (`www.resistoproject.eu/wp-content/uploads/2020/05/Polaris_2020_N41_Aonzo_Neri.pdf`), 2020.

[5] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The Industrial Internet of Things (IIoT): An analysis framework, *Computers in Industry*, vol. 101, pp. 1–12, 2018.

[6] M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace and D. von Winterfeldt, A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra*, vol. 19(4), pp. 733–752, 2003.

[7] M. Bruneau and A. Reinhorn, Exploring the concept of seismic resilience for acute care facilities, *Earthquake Spectra*, vol. 23(1), pp. 41–62, 2007.

[8] E. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan and J. Sterbenz, Modelling communication network challenges for future Internet resilience, survivability, and disruption tolerance: A simulation-based approach, *Telecommunication Systems*, vol. (52), pp. 751–766, 2013.

[9] P. Chopade and M. Bikdash, Critical infrastructure interdependency modeling: Using graph models to assess the vulnerability of smart power grid and SCADA networks, *Proceedings of the Eighth IEEE International Conference and Expo on Emerging Technologies for a Smarter World*, 2011.

[10] G. Digioia, C. Foglietta, S. Panzieri and A. Falleni, Mixed holistic reductionistic approach for impact assessment of cyber attacks, *Proceedings of the IEEE European Intelligence and Security Informatics Conference*, pp. 123–130, 2012.

[11] N. Erez and A. Wool, Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems, *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 59–70, 2015.

[12] I. Eusgeld and W. Kröger, Comparative evaluation of modeling and simulation techniques for interdependent critical infrastructures, Laboratory of Safety

Analysis, ETH Zurich, Zurich, Switzerland, (www.researchgate.net/profile/Wolfgang_Kroeger/publication/293110383_Comparative_evaluation_of_modeling_and_simulation_techniques_for_interdependent_critical_infrastructures/links/57ab796e08ae0932c9713dd4/Comparative-evaluation-of-modeling-and-simulation-techniques-for-interdepe pdf), 2008.

[13] C. Foglietta, D. Masucci, C. Palazzo, R. Santini, S. Panzieri, L. Rosa, T. Cruz and L. Lev, From detecting cyber-attacks to mitigating risk within a hybrid environment, *IEEE Systems Journal*, vol. 13(1), pp. 424–435, 2019.

[14] C. Foglietta, C. Palazzo, R. Santini and S. Panzieri, Assessing cyber risk using the CISIApro Simulator, in *Critical Infrastructure Protection IX*, M. Rice and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 315–331, 2015.

[15] K. Gopalakrishnan and S. Peeta (Eds.), *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, Springer, Berlin Heidelberg, Germany, 2010.

[16] Y. Haimes and P. Jiang, Leontief-based model of risk in complex interconnected infrastructures, *Journal of Infrastructure Systems*, vol. 7(1), pp. 1–12, 2001.

[17] M. Kivelä, A. Arenas, M. Barthelemy, J. Gleeson, Y. Moreno and M. Porter, Multilayer networks, *Journal of Complex Networks*, vol. 2(3), pp. 203–271, 2014.

[18] A. Kwasinski and V. Krishnamurthy, Generalized integrated framework for modelling communications and electric power infrastructure resilience, *Proceedings of the IEEE International Telecommunications Energy Conference*, pp. 99–106, 2017.

[19] D. Masucci, C. Palazzo, C. Foglietta and S. Panzieri, Enhancing decision support with interdependency modeling, in *Critical Infrastructure Protection X*, M. Rice and S. Shenoi (Eds.), pp. 169–183, 2016.

[20] B. Nejad, S. Attia and J. Raisch, Max-consensus in a max-plus algebraic setting: The case of fixed communication topologies, *Proceedings of the Twenty-Second IEEE International Symposium on Information, Communication and Automation Technologies*, 2009.

[21] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety*, vol. 121, pp. 43–60, 2014.

[22] G. Riley and T. Henderson, The ns-3 network simulator, in *Modeling and Tools for Network Simulation*, K. Wehrle, M. Güneş and J. Gross (Eds.), Springer, Berlin Heidelberg, Germany, pp. 15–34, 2010.

[23] S.M. Rinaldi, J.P. Peerenboom and T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, vol. 21(6), pp. 11–25, 2001.

[24] G. Satumtira and L. Dueñas-Osorio, Synthesis of modeling and simulation methods on critical infrastructure interdependencies research, in *Sustainable and Resilient Critical Infrastructure Systems*, K. Gopalakrishnan and S. Peeta (Eds.), Springer, Berlin Heidelberg, Germany, pp. 1–51, 2010.

[25] M. Shafi, A. Molisch, P. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour and G. Wunder, 5G: A tutorial overview of standards, trials, challenges, deployment, and practice, *IEEE Journal on Selected Areas in Communications*, vol. 35(6), pp. 1201–1221, 2017.

[26] U.S. Department of Homeland Security Risk Steering Committee, DHS Risk Lexicon: 2010 Edition, Washington, DC, (`www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf`), 2010.

[27] H. Wang, B. Alidaee and W. Wang, Critical infrastructure management for telecommunication networks, in *Revised Papers from the Eighth International Conference on Active Media Technology*, R. Huang, A. Ghorbani, G. Pasi, T. Yamaguchi, N. Yen and B. Jin (Eds.), Springer, Berlin, Heidelberg, pp. 493–501, 2012.

[28] H. Yang, L. Cheng and M. C. Chuah, Modeling DNP3 traffic characteristics of field devices in SCADA systems of the smart grid, *Proceedings of the IEEE Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2017.

[29] Q. Zhao, Presents the technology, protocols, and new innovations in Industrial Internet of Things (IIoT), in *Internet of Things for Industry 4.0*, G. R. Kanagachidambaresan, R. Anand, E. Balasubramanian and V. Mahima (Eds.), Springer, Cham, Switzerland, pp. 39–56, 2020.