Chapter

# Integrating Resilience in Time-based Dependency Analysis: A Large-Scale Case Study for Urban Critical Infrastructures

*Vittorio Rosato, Antonio Di Pietro, Panayiotis Kotzanikolaou, George Stergiopoulos and Giulio Smedile*

## Abstract

As critical systems shall withstand different types of perturbations affecting their functionalities and their service level, resilience is a very important requirement. Especially in an urban critical infrastructures where the occurrence of natural events may influence the state of other dependent infrastructures from various different sectors, the overall resilience of such infrastructures against large scale failures is even more important. When a perturbation occurs in a system, the quality (level) of the service provided by the affected system will be reduced and a recovery phase will be triggered to restore the system to its normal operation level. According to the implemented recovery controls, the restoration phase may follow a different growth model. This paper extends a previous time-based dependency risk analysis methodology by integrating and assessing the effect of recovery controls. The main goal is to dynamically assess the evolution of recovery over time, in order to identify how the expected recovery plans will eventually affect the overall risk of the critical paths. The proposed recovery-aware time-based dependency analysis methodology was integrated into the CIPCast Decision Support System that enables risk forecast due to natural events to identify vulnerable and disrupted assets (e.g., electric substations, telecommunication components) and measure the expected risk paths. Thus, CIPCast can be valuable to Critical Infrastructure Operators and other Emergency Managers involved in a crisis assessment to evaluate the effect of natural and anthropic threats affecting critical assets and plan proper countermeasures to reduce the overall risk of degradation of services. The proposed methodology is evaluated in a real scenario, which utilizes several infrastructures and Points of Interest of the city of Rome.

**Keywords:** time, resilience, dependency, critical infrastructure, impact, energy, urban, telecommunications, graph, chain, cascading, risk management, risk analysis

## 1. Introduction

Critical infrastructures consist of physical and cyber assets, systems, and networks, that are essential for the functioning of a society and economy. The damage

to a critical infrastructure, caused by natural (e.g., earthquakes, fire) or anthropic (e.g., hacking, sabotage, vandalism) events may produce a significant negative impact for other systems and thus amplify the effects and reducing the system capability to return to an equilibrium state.

In a scenario consisting of multiple infrastructures with several dependencies among them, the implementation of mitigation controls that may affect the resilience level of the systems, is valuable to preserve and restore the essential societal services. Since resilience-related controls will positively affect the capability of a system to resist, absorb, adapt and/or recover from the effects of a hazard in a timely and efficient manner, it is important to analyse the effect of such controls, in order to support decision making related to the selection and prioritization of alternative mitigation controls. For example, when electric transmission or distribution networks are affected by disturbances such as floods, in general, mitigation and restoration actions are performed through protection and automation devices and manual interventions to reduce the duration of the outage and preserve the power supply to critical systems such as hospitals [1–3].

In the US, in order to support the different players involved in modeling, simulation, and analysis of the nation's critical infrastructures, the National Infrastructure Simulation and Analysis Center (NISAC) was established. NISAC analysts assess critical infrastructure risk, vulnerability, interdependencies, and event consequences. In Europe, in order to support the different players involved in the resilience enhancement, emergency and response management of critical infrastructures to natural and man-made hazards, the Infrastructure Simulation and Analysis Centre (EISAC) is aiming at establishing a collaborative, European-wide network of national centres empowered by core technologies.

This paper extends a recent work on critical infrastructure dependency analysis and introduces time-based analysis models to study the evolution of restoration actions in a scenario of dependent systems. This model was integrated into CIPCast Decision Support System, named CIPCast hereafter, that is part of the on-going products and activities developed in the context of the Italian node of EISAC, called I-EISAC, aiming to support infrastructure and civil protection operators operators in the risk assessment of critical infrastructures.

CIPCast can provide an operational (24/7) forecast and risk analysis for different infrastructures in a specific area showing risk maps of infrastructure elements which could be damaged by different events e.g. earthquakes. In particular, CIPCast allows: (i) Assessing the seismic vulnerability of different EDNs components; (ii) estimating possible earthquake-induced physical damage; (iii) estimating the impact on service(s) functionality in terms of outage duration associated with the predicted physical damage and considering the known inter-dependencies; (iv) estimating the consequences of the predicted outages, according to several metrics accounting for economic losses and reduction of citizens well-being.

The remainder of the paper is organized as follows. Section 2 presents related works in the area. In Section 3, we introduce notions of time-based and resilience-aware dependency analysis. In Section 4, we apply the analysis to a case study related to the area of Rome. Finally, in Section 5, some conclusions and ideas for future works are drawn.

## 2. Related work

Modeling critical infrastructures and urban systems for risk assessment purposes is a well-known and established research field. Preliminary work that laid the foundation in this area is often attributed to Rinaldi et al., first in [4] where authors

categorised dependencies in critical infrastructures as Physical, Cyber/informational, Geographic, Logical and Social dependencies, and later in where authors created taxonomies for disruptions or outages and marked them as cascading, escalating, or common-cause [5]). Critical infrastructure modeling events where first defined as cascade initiating (i.e., an event that causes an event in another CI) and cascade resulting (i.e., an event that results from an event in another CI) by the empirical study of Van Eeten et al. [6].

Basic modeling approaches usually fall within one of the following six categories categories [5, 7]:

1. Aggregate supply and demand tools, which evaluate the total demand for infrastructure services in a region and the ability to supply those services

2. Dynamic simulations, which analyze the effects of disruptions, and their associated consequences.

3. Agent-based models, which model operational attributes and states of infrastructure operation; usually on a graph model.

4. Physics-based models, which utilize standard engineering techniques such as power flow and stability analyses for electric power grids.

5. Population mobility models that focus on geospatial movement.

6. Leontief input–output models, which utilize linear, time-independent analysis of commodities among infrastructure sectors.

Our approach can be classified as both dynamic simulation and agent-based model. It utilizes operational attributes to model interdependencies in urban environments as a graph, while still allowing for dynamic input of data in order to analyze the effects of disruptions in the urban web along with quantifying their associated consequences.

Each critical infrastructures sector has its own group of research publications that utilize some of the aforementioned techniques to model and analyse risk. For example, in the water sector, OpenMI [8] supports federated modeling and simulation for water systems, while multiple publications exist that analyze interdependencies at the transportation sector using traffic flow simulation models [9], Bayesian networks to model the correlation structure of highway networks [10] etc. The Energy sector is also a highly researched area. Wide Area Measurement Systems (WAMS) have been extensively researched, especially for the detection of optimal locations for metering device placement, in order to achieve increased robustness of the WAMS infrastructure. Modeling and quantifying dependencies between the electrical and information infrastructures of WAMS in smart grids has been recently studied in [11]. Topological observability of power systems has been fully described in [12]. Still, cross-sector approaches do exist that opt to combine combine models from multiple sectors and enable integrated or federated simulations. Some examples include DIESIS [13] and EPIC [14].

The North American Electric Reliability Corporation (NERC) has recently developed Critical Infrastructure Protection (CIP) standards which introduce cyber security compliance requirements for power systems [15]. Various research has developed methodologies that aim to quantify these requirements. In [15], authors proposed a risk-based dependency analysis for modeling and quantifying dependencies over time, which was also later used in [11] along with electrical centrality

metrics to quantify the level of each dependencies in the smart grid. A different approach for simulating common-cause and cascading effects was also introduced by the authors in [16]. Similarly, authors in [17] proposed to use access graph models to analyze trust between systems and the security exposure of a large scale smart grid environments. In [18], authors developed a graph-based workflow model for assessing the security risks from cybersecurity incidents on electric grids and build relevant scenarios.

The presented approach is mostly based on the methodologies presented in [15]. We aggregate data into dependency matrices and utilize models from real-world urban systems to map them into dependency graphs. The presented approach is based on network modeling and path analysis. It depicts dependencies of the connected urban infrastructures as a graph and identifies high risk, critical paths that are either modeled as flows of information, power or other related type of dependency. Similar techniques have been used in uniform [19, 20] or flow models [12, 21].

## 3. Time-based and resilience-aware dependency analysis

### 3.1 Definitions and set up

We consider a directed graph $G = (V, E)$ where $V = \{v_i\}$, $i = 1, \ldots m$, is the set of nodes (infrastructures, components or Point of Interest–POIs hereafter) and $E = \{e_{ij}\}$ is the set of edges (or dependencies) and $deg(v_i)$ is the degree of node $v_i$. An edge $e_{ij}$ from node $v_i$ to $v_j$ denotes a dependency (and consequently a risk relation) denoted with $v_i \rightarrow v_j$ that is derived from the dependence of node $v_j$ on a service provided by node $v_i$. A dependency is defined as a "one-directional reliance of an asset, system, network or collection thereof – within or across sectors – on an input, interaction or other requirement from other sources in order to function properly" [22]. A node could thus represent a *consumer* or a *producer* of a service provided by another node (or both), depending on its role in the system.

Our model extends the cumulative dependency risk model of [23, 24]. Without loss of generality, let $v_0 \rightarrow v_1 \rightarrow \ldots \rightarrow v_n$ be a dependency chain, involving $n+1$ nodes and their corresponding $n$ dependencies. Let $L_{v_{j-1},v_j}$ be the likelihood that a disruptive event (threat) that happened in node $v_{j-1}$ will also affect (cascade) to node $v_j$ due to their dependency and let $I_{v_{j-1},v_j}$ be the relevant impact (damage) caused to $v_j$. We should note here that $L$ is not the likelihood of threat manifestation, but rather the likelihood of an already manifested threat to cascade (i.e. affect) different nodes.

Based on the definitions of [23], the risk exhibited by a node due to its $n$-th order dependency is defined as:

$$R_{v_0,\ldots,v_n} = L_{v_0,\ldots,v_n} \cdot I_{v_{n-1},v_n} \equiv \prod_{i=0}^{n-1} L_{v_i,v_{i+1}} \cdot I_{v_{n-1},v_n}. \tag{1}$$

Then the *cumulative dependency risk* which includes the *overall* risk exhibited by all the nodes within the sub-chains of an $n$-order dependency is defined as:

$$DR_{v_0,\ldots,v_n} = \sum_{i=1}^{n} R_{v_0,\ldots,v_i} \equiv \sum_{i=1}^{n} \left( \prod_{j=1}^{i} L_{v_{j-1},v_j} \right) \cdot I_{v_{i-1},v_i}. \tag{2}$$

### 3.2 Extending the model for resilience

Let $\mathbb{T} = \{threat\}$ be the set of $k$ natural or human-related threats that may affect the quality of service provided by the generic node $v_i$. The damage $D_i(t)$ associated with the perturbation $t$ is usually an s-shaped function. Let $\mathbb{C}^{v_i} = \left\{c_1^{v_i}, \ldots, c_l^{v_i}\right\}$ be the set of $l^{v_i}$ security controls that may be implemented in a system/infrastructure $v_i$ to improve their resilience against threats (e.g. restoration security controls, redundancy security controls etc).

By combining Resilience and Threat variables with the directed graph model of interdependent POIs, we can perform a granular analysis of the risk imposed by POI interdependencies based on their risk and resilience levels. We opt to use the multi-risk dependency analysis method as proposed in [23–25] and implemented later in [15].

### 3.3 Resilience mapping

A many-to-many mapping may exist between the threats and the security controls, i.e. a security control may mitigate, at some extent, one or more threats, while a security threat may require one or security controls. For each security control, different weights can be used to define the effectiveness of a control against different threats and also for their application to specific infrastructures. This is a realistic modeling of resilience, since many controls do not have the same effect against all threats and different infrastructures are benefited more than others from specific security controls, given the nature of the infrastructure and the intrinsic characteristics of each threat.

For example, if infrastructure (node) $v_1$ is affected by a power outage (i.e. the initiating threat event), then a node $v_2$ which is depended on $v_1$ might suffer a partial unavailability (modeled as impact $I_{v_1,v_2}$) at a certain extend quantified as the likelihood $L_{v_1,v_2}$. $L_{v_1,v_2}$ depicts the possibility that a power outage would affect node $v_2$ and $I_{v_1,v_2}$ depicts the amount of damage done to $v_2$ due to its partial unavailability incident.

In the aforementioned example, node $v_1$ could have implemented the use of a redundant power generator as a security control with quantified measurements (i) $\overline{L}_{v_1,v_2}$ and (ii) $\overline{I}_{v_1,v_2}$ depicting (i) the resilience influence of control $c$ on node $v_2$ for the given threat (in our case, the power outage), and (ii) the extent of reduction to the initial estimated damage $I_{v_1,v_2}$, respectively. The existence of the control $c$ will reduce the possibility of a power outage to affect $v_2$ by $\overline{L}_{v_1,v_2}$ percent, and/or the corresponding impact from the same threat on $v_2$ by $\overline{I}_{v_1,v_2}$.

Generalising this to $n$ nodes, this gives us with a Resilience series calculation that can be depicted as follows:

$$Res_{v_0,\ldots,v_n} = \sum_{i=1}^{n}\left(\prod_{j=1}^{i}\overline{L}_{v_{j-1},v_j}\right)\cdot\overline{I}_{v_{i-1},v_i} \tag{3}$$

where *Res* depicts the overall resilience of a network against a specific $threat \in \mathbb{T}$ when the security control $c$ is implemented in all nodes. It should be noted, that the resilience expressed by Eq. (3) depicts the resilience of a network due to the existence and the efficacy of security control $c$. However, the Resilience of a network depends also on the vulnerability of the node $v_j$ to specific threats that may produce a disservice of the network.

For example, if we consider an electric substation, in order to increase its resilience against a seismic threat, there might be several options aiming to reduce the likelihood of the threat that produces a failure and/or to reduce the magnitude of

the impact e.g. to enhance the structural properties of the building or increment the number of technical crews so that in case of a failure the duration of outage can be reduced.

In a complex study of a large CI system, such as the city of Rome, the interplay among network topology, size, quality and distribution of technical systems along the network, emergency management ability do have an impact on the evolution and the duration of a crises and thus influence the system resilience. They have been thus studied in order to establish the "sensitivity" of the resilience score with respect to each one of the described properties [3].

Conveniently, the Resilience introduced by a security control against a specific threat on the entire network of interdependent nodes can be algorithmically modeled as a matrix multiplication. For the first matrix, columns represent existing nodes, while rows represent different security controls. Cell values depict the possibility of a security control to mitigate some part of the impact of a specific threat for each node present in the graph. The second matrix depicts the impact reduction that can be achieved by security controls onto the existing interdependent nodes. Similarly, columns represent existing nodes, while rows represent different security controls, but, here cell values depict the maximum potential impact reduction achieved at each node by the implementation of each security control. Thus, in this matrix, cells have negative values. Resilience is then modeled as the matrix multiplication of the two matrices (threat reduction and impact reduction matrices), as depicted in **Figure 1**.

### 3.4 Calculating cumulative dependency risk in the presence of resilience controls

By combining Eq. 1 and Eq. 2 with Eq. 3, the cumulative dependency risk in the presence of resilience controls can be defined as follows:

$$DR^{Res}_{v_1,\ldots,v_n} = \sum_{i=1}^{n}\left[\left(\prod_{j=1}^{i} L_{v_{j-1},v_j}\right)\cdot I_{v_{i-1},v_i} - \left(\prod_{j=1}^{i} \overline{L}_{v_{j-1},v_j}\right)\cdot \overline{I}_{v_{j-1},v_j}\right] \qquad (4)$$

As discussed above, $\overline{L}_{v_{j-1},v_j}$ introduces a likelihood for the security controls (actions). Specifically, it quantifies the possibility of one security control to mitigate some part of the impact of a threat.

Impact $I$ in Eqs. 1 through 4 is assigned values that reflect the maximum expected impact for each modeled dependency. This first implies that eqs will always calculate produce the worst case cascading risk $DR^{Res}_{v_1,\ldots,v_n}$, and also that all modeled dependencies exhibit the same impact growth rate; something that is not true in real-world situations, where different infrastructure resilience allows for different impact growth rates over time. Thus, we use the same modeling approach as in [15] and incorporate a dynamic time-based analysis model where $T_{i,j}$ denotes

| Likelihood matrix for Threat *(threat)* | | | | |
|---|---|---|---|---|
| Nodes / Controls | $v_1$ | $v_2$ | … | $v_n$ |
| $c_1$ | 0,34 | 0,23 | … | 0,18 |
| $c_2$ | 0,12 | 0,41 | … | 0,21 |
| . | … | … | … | … |
| . | … | … | … | … |
| $C_n$ | 0,19 | 0,08 | … | 0,6 |

+

| Likelihood matrix for Threat *(threat)* | | | | |
|---|---|---|---|---|
| Nodes / Controls | $c_1$ | $c_2$ | … | $c_n$ |
| $v_1$ | -3 | -6 | … | -4 |
| $v_2$ | -1 | -3 | … | -3 |
| . | … | … | … | … |
| . | … | … | … | … |
| $v_n$ | -5 | -2 | … | -2 |

=

| Resilience against *(threat)* | | | | |
|---|---|---|---|---|
| Nodes / Controls | $v_1$ | $v_2$ | … | $v_n$ |
| $c_1$ | -2,15 | | | |
| $c_2$ | | | | |
| . | | | | |
| . | | | | |
| $C_n$ | | | | |

**Figure 1.**
*Resilience security control calculation for the entire network against a single threat* $\in \mathbb{T}$.

the time period over which a dependency between two infrastructures exhibits its maximum expected impact $I_{i,j}$, and $G_{i,j}$ denotes the expected growth of the failure. The growth rates used in this model are split into three types, namely: slow, linear or fast. Finally, let $t$ denote an examined time period after a failure.

Growth rates $G_{i,j}$ are defined based on the maximum potential Impact $I_{i,j}$ and a growth relation between time step $t$ and $T_{i,j}$. Specifically, "slow" growth rates follow a exponential evolution of type

$$I(t) = I^{\frac{t}{T}} \tag{5}$$

which begins at a slow pace and gradually increases in speed. "Linear" growth rates follow a typical approach

$$I(t) = I \cdot \frac{t}{T} \tag{6}$$

whereas "fast" impact growth rates are calculated using a logarithmic approach

$$I(t) = I \cdot \log_T t \tag{7}$$

in which incidents impose a very fast impact growth rate that gradually decreases in speed. For any $t >= T$, impact growth caps at $I(t) = I$.

In real-world implementations of the methodology, all aforementioned values for $T_{i,j}$ and $G_{i,j}$, along with $I_{i,j}$ and $L_{i,j}$, are obtained through on-site assessment, expert knowledge and quantification of infrastructure characteristics.

### 3.5 Qualitative ranking scales

The above equations need some sort of value ranges in order to quantify results. To support calculation of these equations, we opted to use the same scales as in [15]. All the values are assigned from the following Likert scales:

- $I \epsilon [1..9]$, where 1 is the lowest impact and 9 is the highest impact.
- $T, t \epsilon [1..10]$, which is a granular time scale that uses the unavailability time periods: 1 = 15 min, 2 = 1 h, 3 = 3 h, 4 = 12 h, 5 = 24 h, 6 = 48 h, 7 = 1w, 8 = 2w, 9 = 4w and 10 = more than 4w.
- $G \epsilon [1..3]$, where the value of 1 represents the slow growth rate, and values (2) and (3) represent the linear and fast evolution rates for impact respectively.

Each Impact value reflects a different qualitative criterion, based on the needs and threats of any given infrastructure. Nevertheless, quantification is uniform amongst all possible implementations, where a value of 1 reflects minimum to no Impact, while a value of 9 reflects catastrophic impact of an incident.

## 4. Case study: City of Rome

The city center of Rome was chosen as a case study due to the high concentration of various commercial activities and power centres both local and international as well as the presence of CIs which are essential to maintain vital societal functions (**Figures 2** and **3**). In particular, the area of interest holds the major Italian

government offices, *San Giovanni Calibita Fatebenefratelli Hospital* located in the Tiber Island and *Termini Railway Station*, one of the most important railway stations of Italy as it connects Northern and Southern Italy.

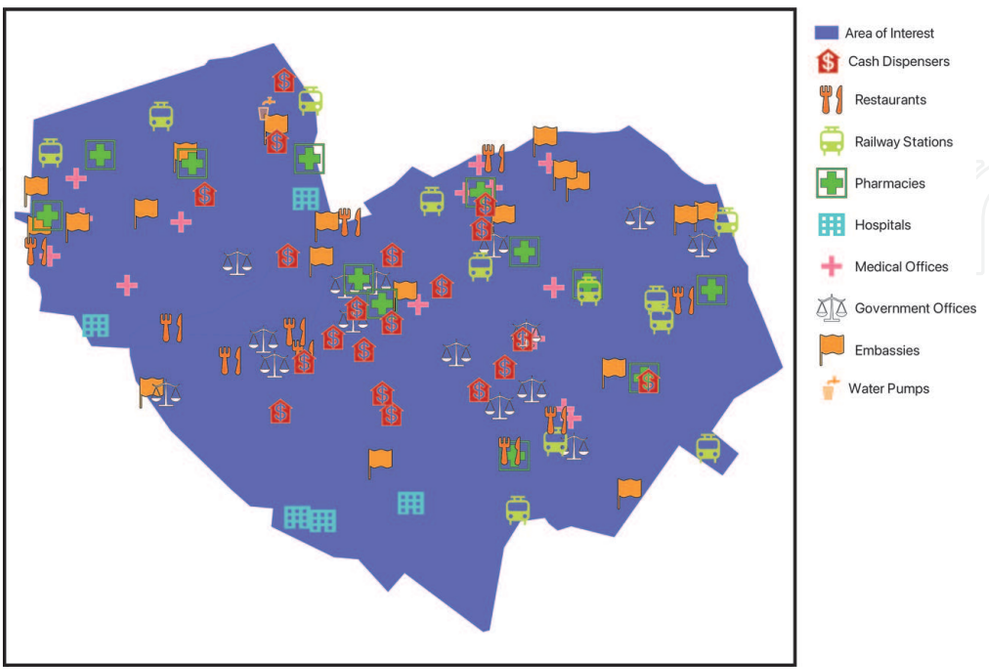


**Figure 2.**
*The area of interest: an urban district of Rome. The map was anonymized and MV Electric substations and Base Transceiver Stations were removed to hide sensitive information.*

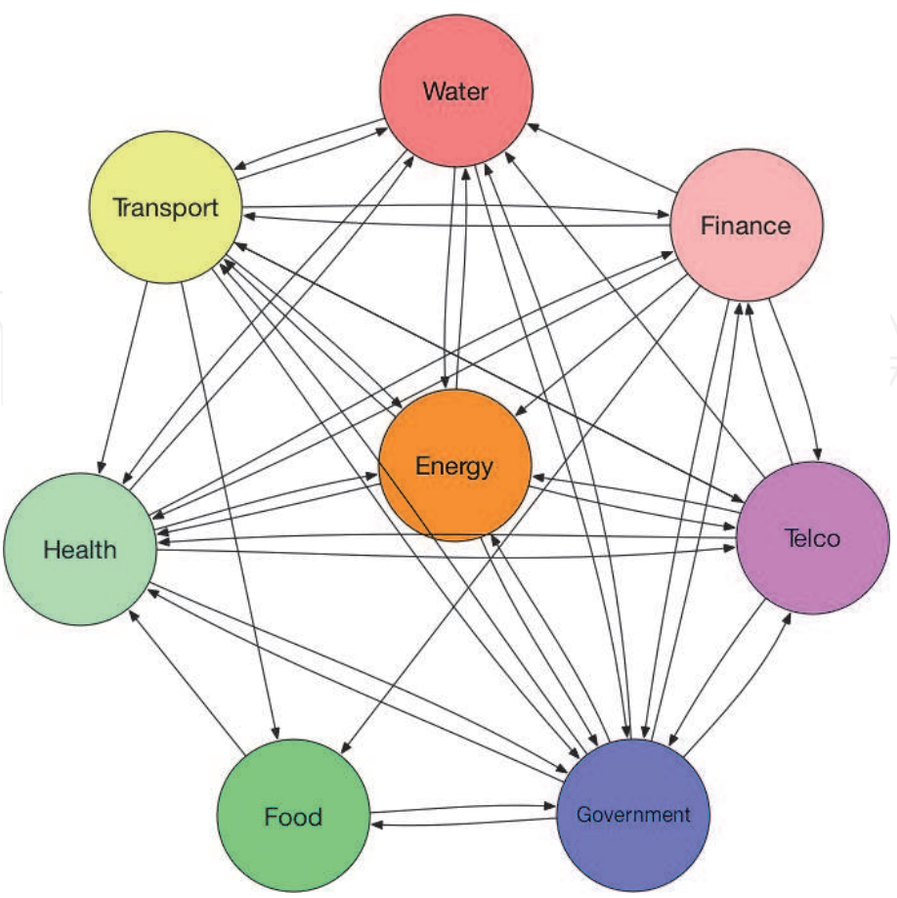


**Figure 3.**
*The dependency graph used in the case study.*

As reported in **Table 1**, we considered 8 categories including CI and Point of Interests and selected a set of specific components (nodes, hereafter) for each category that are located in the area of interest. In particular, we considered the following categories:

i. the Electric Distribution Network (EDN) of Rome consisting of 40 Medium Voltage (15 kV) substations;

ii. the Mobile Telecommunication System consisting of 31 Base Transceiver Stations (BTS);

iii. the Water Supply Network (WSN) consisting of 1 water pumping station;

iv. the Railway system including 12 stations;

v. a set of hospitals, medical offices and pharmacies;

vi. a set of government offices and embassies;

vii. a set of cash dispensers;

viii. a set of restaurants.

### 4.1 Dependency graph

In order to model the interdependencies among the different nodes, we assumed a cyber risk assessment as the case scenario. In particular, we considered a *dependency matrix* [26] that allows to reveal the potential vulnerability of a given node to the unavailability, corruption or disclosure of data from an interdependent node regardless of the current state of the shared data infrastructure. In other words, we assume a cyber threat $threat \in \mathbb{T}$ affecting the considered nodes and we use a *precomputed* dependency matrix as a means to assign a cyber vulnerability to each node w.r.t. the data disruption from all interdependent nodes.

| Category | Subcategory | Acronym | Nr. |
|---|---|---|---|
| Energy | MV Electric substation | ES | 40 |
| Telecommunications | Base Transceiver Station | BTS | 31 |
| Finance | Cash Dispenser | CD | 20 |
| Government | Government Office | GO | 15 |
| | Embassy | EM | 20 |
| Transport | Railway Station | RS | 12 |
| Health | Medical Office | DO | 15 |
| | Pharmacy | PH | 12 |
| | Hospital | HP | 5 |
| Food | Restaurant | RE | 10 |
| Water | Water Pumping station | WP | 1 |
| **Total:** | | | 182 |

**Table 1.**
*CI categories and components modeled in the case study.*

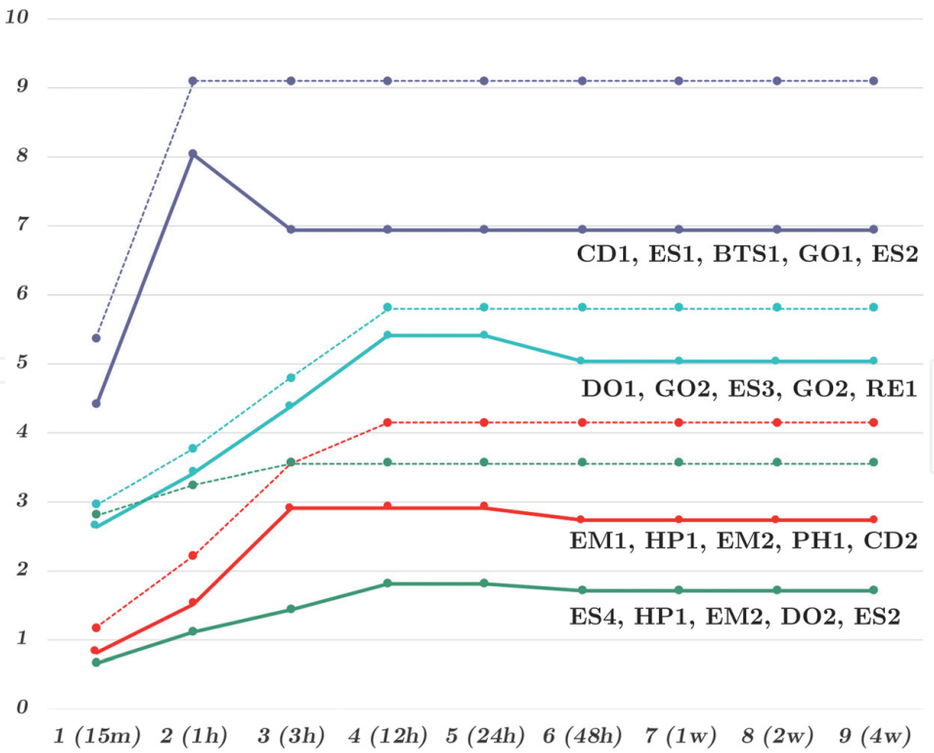


**Figure 4.**
*A set of dependency risk paths with cumulative dependency risk. Dashed/continuous lines indicate the risk without/with the implementation of security controls.*

The dependency matrix is consistent with the main cyber interdependencies that exist among the nodes modelled in the scenario although only a limited number of CI were considered for each sector present in the dependency matrix. Indeed, the electric substations (ES) supply energy to all nodes of other CI and thus a failure occurring in an ES would be disruptive for all nodes that receive energy from that ES. In addition, some of the ES are Remotely controlled and thus a failure occurring in those BTS nodes that in turn provide telecommunication services to the Remotely Controlled ES may compromise the control operations of the EDN.

In the absence of information regarding specific interdependencies, we employed a proximity criterion to model the relations among specific nodes. For example, we assumed that each energy consumer (i.e., all nodes that are not ES) is supplied by the nearest ES as well as each internet/telephony consumer is supplied by the nearest BTS. In addition, we did not model the intra-sector dependencies i.e. any dependency among the nodes of the same CI sector was not considered.

### 4.2 Likelihood matrix

As described previously, we employed the dependency matrix defined in [26] to model the interdependencies of the case study. That matrix was filled by gathering over 4.000 distinct data dependency metrics from CI stakeholders and reports the same CI sectors that were modelled in the case study and the cyber vulnerability of each sector w.r.t. all CI sectors. **Table 2** shows the value for both Inbound and Outbound data dependencies. Inbound data dependency represents information and data consumed by the examined CIs, while outbound data dependency represents the data leaving each examined CI, to be used by other CIs.

The columns for each sector represent how that sector is dependent by data coming into that sector. Most organisations can intuitively estimate this value, and that's how the data was collected in [26]. For example, in **Table 2**, column *BTS* represents the data, informations and services any BTS station would receive from

each other sector, and how much that BTS station depends from that data, information or service.

Based on this matrix, we normalised the values and neglected the intradependencies and the low intradependencies. In other words, we treated the cyber vulnerability of a node as a likelihood that the node being affected. The resulting matrix is shown in **Table 2**.

### 4.3 Security Controls

Given the absence of information regarding the security controls implemented by the considered nodes, we assumed that each node $v_i$ having a dependency with $v_j$ where $j \in \{1, .., N_i\}$, is equipped with $l^{v_i}$ security controls against the examined *threat*. We assumed that the likelihood values of the restoration controls $\overline{L}_{v_i,v_j} = const. \forall j \in \{1, .., N_i\}$. **Table 3** shows the likelihood values of the restoration controls.

### 4.4 Impact Assessment Criteria

In order to assess the impact of cyber attacks on the nodes, we considered the work of Fekete [27] that defines three impact assessment criteria in terms of critical proportion, time and quality aspects. Critical proportion refers to the number of elements or nodes of a CI such as critical number of services, size of population or number of customers affected and redundancies. Critical time considers aspects such as duration of outage, Mean Time to Repair (MTTR), Mean Time to Functionality (MTTF) and business continuity or interruption. Critical quality refers to the quality of the services delivered (e.g., the water quality) or the public trust in quality (e.g., trust in finance, feeling of security).

In the following subsections, a description of how the mentioned impact assessment criteria were applied to the case study will be provided. In particular, the assumptions that were made to take into account such criteria will be described in order to model the expected time-related impact $I(t)$ in terms of the maximum expected impact $I$, the impact time $T$ and the impact growth rate $G$, as defined in Section 3.

| | **Inbound Dependencies** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **CI Sector** | **ES** | **BTS** | **CD** | **GO** | **EM** | **RS** | **DO** | **PH** | **HP** | **RE** | **WP** |
| **ES** | — | 0.36 | — | 0.34 | 0.34 | 0.43 | 0.39 | 0.39 | 0.39 | — | 0.31 |
| **BTS** | 0.7 | — | 0.45 | 0.4 | 0.4 | 0.44 | 0.51 | 0.51 | 0.51 | — | 0.34 |
| **CD** | 0.71 | 0.72 | — | 0.4 | 0.4 | 0.4 | 0.42 | 0.42 | 0.42 | 0.44 | 0.5 |
| **GO** | 0.59 | 0.51 | 0.7 | — | — | 0.36 | 0.61 | 0.61 | 0.61 | 0.36 | 0.51 |
| **EM** | 0.59 | 0.51 | 0.7 | — | — | 0.36 | 0.61 | 0.61 | 0.61 | 0.36 | 0.51 |
| **RS** | 0.68 | 0.4 | 0.42 | 0.29 | 0.29 | — | 0.5 | 0.5 | 0.5 | 0.51 | 0.3 |
| **DO** | 0.41 | — | 0.3 | 0.51 | 0.51 | — | — | — | — | — | 0.44 |
| **PH** | 0.41 | — | 0.3 | 0.51 | 0.51 | — | — | — | — | — | 0.44 |
| **HP** | 0.41 | — | 0.3 | 0.51 | 0.51 | — | — | — | — | — | 0.44 |
| **RE** | — | — | — | 0.27 | 0.27 | — | 0.38 | 0.38 | 0.38 | — | — |
| **WP** | 0.49 | — | — | 0.29 | 0.29 | 0.32 | 0.36 | 0.36 | 0.36 | — | — |

**Table 2.**
*The likelihood matrix used in the case study.*

| $v_i$ | $\overline{L}_{v_i,v_j}$ |
|---|---|
| ES, BTS, CD, GO, EM | 0.3 |
| RS, HP, WP | 0.1 |
| DO, PH, RE | 0 |

**Table 3.**
*Resilience influence of security control $c^{v_i}$ on node $v_j$ for the given threat with dependency risk subchain $v_i \rightarrow v_j$.*

### 4.4.1 Maximum expected impact matrix

In order to apply the critical proportion criterion, given the difficulty of obtaining the number of customers supplied by a specific node from the CI owners, we assumed the number of inhabitants living in the geographical area where the specific node is located as the number of customers. Indeed, the areas considered are the census areas delivered by the *Italian National Institute of Statistics* (ISTAT) of which the number of inhabitants is known. This criterion was applied to model the maximum expected impact $I$ for each couple of nodes $i$ and $j$ belonging to Energy, Telecommunication, Transport and Finance sectors. Thus, $I$ was computed by combining the total number of customers supplied by $i$ and $j$ nodes so that the more customers are involved in the disruption of the nodes, the more impact we obtain.

Furthermore, the critical quality criterion was applied to compute $I$ for each couple of nodes $i$ and $j$ belonging to Government, Health, Food and Water. In this case, we set a subjective value that takes into account the importance of the unavailability of the data for the specific nodes.

**Table 4** summarises the criteria applied based on the sector nodes considered. It should be noticed that while $I$ is time dependent when considering ES, BTS, RS and CD nodes (case $A$), this is not true when considering GO, EM, DO,PH, HP and RE nodes (case $B$) where $I$ was set higher for the nodes that could be more impacted by the lack of data services. For case $C$, the two criteria were both considered and $I$ was computed according to the metric reported in **Table 4**. The resulting impact matrix is shown on **Table 5**.

Let $v_0, v_1, .., v_n$ be a subchain of risk. We assumed that the reduction of impact $\overline{I}_{v_{i-1},v_i}$ on node $v_i$ due to the restoration action $c^{v_{i-1}}$ implemented by $v_{i-1}$ is given by:

$$\overline{I}_{v_{i-1},v_i} = \alpha \cdot I_{v_{i-1},v_i} \tag{8}$$

**Table 6** shows the percentage of reduction $\alpha$ of the initial estimated damage $I_{v_{i-1},v_i}$ for the generic dependency risk subchain $v_{i-1} \rightarrow v_i$.

### 4.4.2 Impact time and Impact growth rate matrices

Regarding the critical time criterion, we considered the expected duration of failure of nodes to compute the impact and growth time matrices. In particular, we assigned a low value to sectors that are highly dependent on the data availability and

| Case | $v_j$ | Impact assessment criterion | $I_{v_i,v_j}$ |
|---|---|---|---|
| A | ES, BTS, RS, CD | Nr. of customers | node-dependent |
| B | GO, EM, DO, PH, HP, RE | Service criticality | sector-dependent |

**Table 4.**
*Maximum expected impact criteria for the dependency risk subchain $v_{i-1} \rightarrow v_i$.*

| | Inbound dependencies | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **CI Sector** | **ES** | **BTS** | **CD** | **GO** | **EM** | **RS** | **DO** | **PH** | **HP** | **RE** | **WP** |
| **ES** | — | ⋆ | — | 7 | 4 | ⋆ | 4 | 4 | 7 | — | 7 |
| **BTS** | ⋆ | — | ⋆ | 7 | 4 | ⋆ | 3 | 3 | 6 | — | 6 |
| **CD** | ⋆ | ⋆ | — | 3 | 2 | 2 | 2 | 2 | 4 | 2 | 2 |
| **GO** | 8 | 8 | 3 | — | — | ⋆ | 3 | 3 | 5 | 3 | 5 |
| **EM** | 4 | 4 | 2 | — | — | 3 | 2 | 2 | 4 | 2 | 4 |
| **RS** | ⋆ | ⋆ | 2 | ⋆ | 3 | — | 3 | 3 | 4 | 3 | 3 |
| **DO** | 2 | — | 2 | 3 | 2 | — | — | — | — | — | 3 |
| **PH** | 2 | — | 2 | 3 | 2 | — | — | — | — | — | 3 |
| **HP** | 7 | — | 4 | 5 | 4 | — | — | — | — | — | 5 |
| **RE** | — | — | — | 3 | 2 | — | 2 | 2 | 2 | — | — |
| **WP** | 3 | — | — | 3 | 3 | 3 | 3 | 3 | 3 | — | — |

**Table 5.**
*Maximum expected impact matrix used in the case study. ⋆ represents node-dependent impact.*

| $v_{i-1}$ | $v_i$ | $\alpha$ |
|---|---|---|
| ES, BTS | any | 0.5 |
| CD, GO, EM, RS, DO, PH, HP, RE, WP | any | 1 |

**Table 6.**
*Percentage of reduction $\alpha$ of the initial estimated damage $I_{v_{i-1},v_i}$ for the dependency risk subchain $v_{i-1} \rightarrow v_i$.*

that produce a quick impact such as Energy and Telecommunication and Finance and assigning a higher value to other sectors such as Water and Food that produce their negative effect in a longer period. The resulting impact time matrix is shown on **Table 7**.

Regarding the recovery time matrix, we modeled a time $\overline{T} = 15m$ for the electric substations ES are remotely controled as the SCADA system of the electric network allows to reactivate the electric supply in the order of minutes whereas $\overline{T} = 1h$ for a generic ES only a manual intervention performed by a repair crew can be operated with a longer time (approximately 1 hour). The resulting recovery time matrix is shown on **Table 8**.

Regarding the impact growth rate, **Table 9** shows the the criterion adopted and **Table 10** shows the resulting values for each couple of nodes. We considered the same growth rate for the recovery actions.

### 4.5 Results

The execution of the model based on the graph of 182 nodes produced about 750.000 risk paths with order ranging from five to eight and potential risk values between 0.27 and 9.53. **Figure 4** shows some significant dependency paths together with their cumulative dependency risk values.

The charts show that one dependency path ($CD_1$-$ES_1$-$BTS_1$-$GO_1$-$ES_2$) exhibits its highest risk value at time $t = 1h$ and then the implementation of mitigation strategies with a rapid response decreases the overall dependency risk. In general,

| | Inbound dependencies | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **CI Sector** | **ES** | **BTS** | **CD** | **GO** | **EM** | **RS** | **DO** | **PH** | **HP** | **RE** | **WP** |
| **ES** | — | 3 h | — | 3 h | 3 h | 3 h | 3 h | 3 h | 3 h | — | 24 h |
| **BTS** | 3 h | — | 1 h | 3 h | 3 h | 3 h | 3 h | 3 h | 3 h | — | 3 h |
| **CD** | 3 h | 3 h | — | 3 h | 3 h | 3 h | 12 h | 12 h | 3 h | 2w | 24 h |
| **GO** | 3 h | 3 h | 3 h | — | — | 12 h | 12 h | 12 h | 12 h | 2w | 24 h |
| **EM** | 3 h | 3 h | 3 h | — | — | 12 h | 12 h | 12 h | 12 h | 2w | 24 h |
| **RS** | 3 h | 3 h | 3 h | 12 h | 12 h | — | 12 h | 12 h | 12 h | 2w | 24 h |
| **DO** | 3 h | — | 3 h | 24 h | 24 h | — | — | — | — | — | 24 h |
| **PH** | 3 h | — | 3 h | 24 h | 24 h | — | — | — | — | — | 24 h |
| **HP** | 3 h | — | 3 h | 24 h | 24 h | — | — | — | — | — | 24 h |
| **RE** | — | — | — | 2w | 2w | — | 2w | 2w | 2w | — | — |
| **WP** | 24 h | — | — | 24 h | 24 h | 24 h | 24 h | 24 h | 24 h | — | — |

**Table 7.**
*The maximum impact time matrix used in the case study.*

| | Inbound dependencies | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **CI Sector** | **ES** | **BTS** | **CD** | **GO** | **EM** | **RS** | **DO** | **PH** | **HP** | **RE** | **WP** |
| **ES** | — | 15 m | — | 15 m | 15 m | 15 m | 15 m | 15 m | 15 m | — | 15 m |
| **BTS** | 3 h | — | 1 h | 1 h | 1 h | 1 h | 1 h | 1 h | 1 h | — | 1 h |
| **CD** | 3 h | 3 h | — | 3 h | 3 h | 3 h | 12 h | 12 h | 3 h | 2w | 24 h |
| **GO** | 3 h | 3 h | 3 h | — | — | 12 h | 12 h | 12 h | 12 h | 2w | 24 h |
| **EM** | 3 h | 3 h | 3 h | — | — | 12 h | 12 h | 12 h | 12 h | 2w | 24 h |
| **RS** | 3 h | 3 h | 3 h | 12 h | 12 h | — | 12 h | 12 h | 12 h | 2w | 24 h |
| **DO** | 3 h | — | 3 h | 24 h | 24 h | — | — | — | — | — | 24 h |
| **PH** | 3 h | — | 3 h | 24 h | 24 h | — | — | — | — | — | 24 h |
| **HP** | 3 h | — | 3 h | 24 h | 24 h | — | — | — | — | — | 24 h |
| **RE** | — | — | — | 2w | 2w | — | 2w | 2w | 2w | — | — |
| **WP** | 24 h | — | — | 24 h | 24 h | 24 h | 24 h | 24 h | 24 h | — | — |

**Table 8.**
*The maximum recovery time matrix used in the case study.*

| | | **Growth rate node *i*** | | |
|---|---|---|---|---|
| ***G*** | | **Slow** | **Linear** | **Fast** |
| Growth rate node *j* | **Slow** | Slow | Slow | Linear |
| | **Linear** | Slow | Linear | Fast |
| | **Fast** | Linear | Fast | Fast |

**Table 9.**
*Impact growth rate metric.*

| | Inbound dependencies | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **CI Sector** | **ES** | **BTS** | **CD** | **GO** | **EM** | **RS** | **DO** | **PH** | **HP** | **RE** | **WP** |
| **ES** | — | F | — | F | F | F | F | F | F | — | L |
| **BTS** | F | — | L | L | L | L | L | L | L | — | S |
| **CD** | F | L | — | L | L | L | L | L | L | L | S |
| **GO** | F | L | L | — | — | L | L | L | L | L | S |
| **EM** | F | L | L | — | — | L | L | L | L | L | S |
| **RS** | F | L | L | L | L | — | L | L | L | L | S |
| **DO** | F | — | L | L | L | — | — | — | — | — | S |
| **PH** | F | — | L | L | L | — | — | — | — | — | S |
| **HP** | F | — | L | L | L | — | — | — | — | — | S |
| **RE** | — | — | — | S | S | — | S | S | S | — | — |
| **WP** | L | — | — | S | S | S | S | S | S | — | — |

**Table 10.**
*The impact growth rate matrix used in the case study.*

we observed an high risk value of subchains including the electric nodes due both to the high number of dependencies of nodes on the electric nodes and the high maximum impact associated.

**Figure 5** shows a map representation of the dependency risk paths considered in **Figure 4** with the census areas involved. In particular, let $CA_1, CA_2, .., CA_M$ be the set of generic census area containing the CI nodes of all possible dependency chains. The generic $CA_k$ s.t. $1 \leq k \leq M$, $CA_k = \{v_j\}$, $|CA_k| \leq n$ is associated specific a color according to the cumulative risk value $DR^k_{v_0,\ldots,v_n}$ of a $v_0, v_1, .., v_n$ dependency subchain s.t. $\nexists$ a $p_0, p_1, .., p_g$ dependency chain s.t. $DR^k_{v_0,\ldots,v_n} < DR^k_{p_0,\ldots,p_g}$ with some

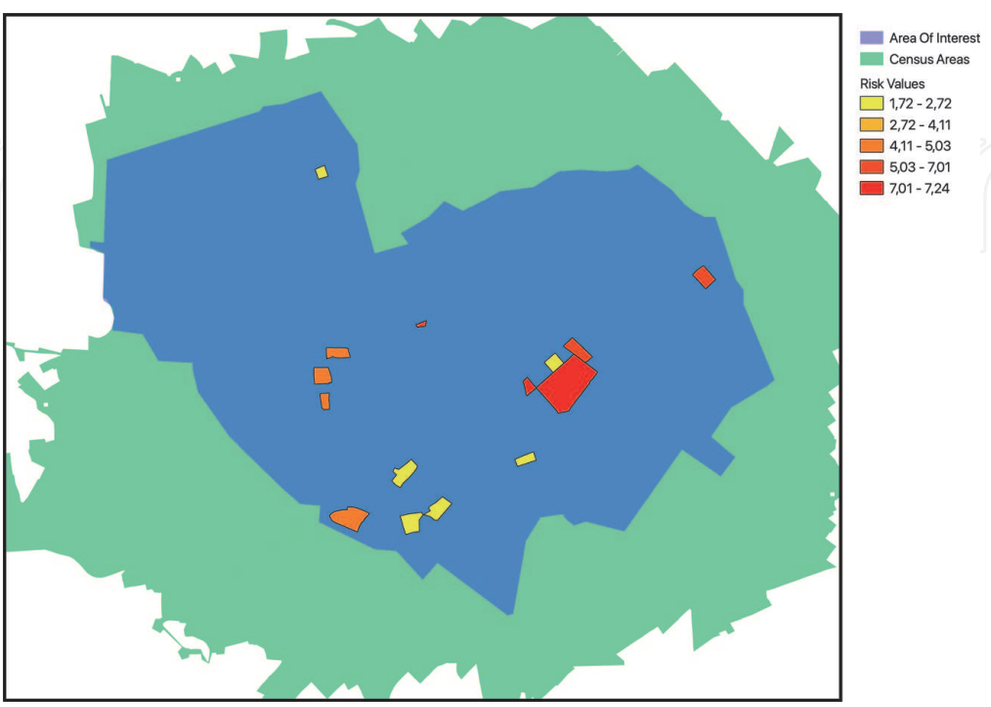


**Figure 5.**
*Result map showing the risk value of each census area.*

$p_h \in CA_k$ $(0 \leq h \leq g)$. In other words, each census area is colored according to the maximum risk value of a subchain that includes some nodes $v_j$ that are located in that area (i.e. $v_j \in CA_k$).

Results depicted in **Figure 4** indicate cascading events between infrastructures. Each one of the four scenarios was validated to be true against real world data and historical analysis of such infrastructures. Following this, results indicate that the presented methodology is able to both (i) effectively project adverse effects from cascading events and accurately predict potential impact over time periods, and also (ii) highlight direct and indirect dependency vulnerabilities between highly dependent CIs.

On the latter, results delineate the criticality behind dependencies of Telecommunications and the Electrical sector. The sharp increase in impact over a very short time period (purple line, scenario 1) clearly shows that potential unavailability of the Electrical sector quickly and critically affects the Telecommunications. We followed up on this finding and results are proven true both from empirical analysis and also from historical data on locations analyzed by the tool.

Another potential use of the presented methodology includes capturing the effect of applying security controls and how these controls affect the resilience of systems over time. By analyzing the impact escalation and trajectory in analyzed attack paths, we see that the level of risk reduction for each of the presented scenarios is directly related with the time of deployment. Early application of security controls (scenario CD1, ES1, BTS1, GO1, ES2) seems to reduce the overall risk by 25% in less than two hours after the initiation of the attack path, while controls implemented later during the exposure to the adverse event show relatively smaller mitigation percentages of the overall risk (around 18%).

Red areas shown in **Figure 5** are highly populated areas containing electric nodes thus producing possible high impact in case of failure. This explains why several nodes of the subchains with high cumulative dependency risk are concentrated in this area.

## 5. Conclusions

By extending previous time-based dependency analysis models and by integrating the effect of resilience-related security controls, in this paper we have examined the effect of possible mitigation strategies in dynamically reducing the consequences of cascading effects. The model was applied to a real case study involving an urban area of Rome where a number of critical infrastructures deliver services to inhabitants and businesses. The model was set up by considering a precomputed dependency graph that exhibits the cyber dependencies of a set of infrastructures. The results highlight the most critical dependency chains and the areas with high concentration of critical nodes. The model was integrated into CIPCast Decision Support System allowing all actors involved in securing critical infrastructures to plan mitigation strategies aiming at reducing the overall risk of service degradation in the considered area.

## Acknowledgements

Authors wish to acknowledge the funding of project RAFAEL (MIUR ARS01_00305) which has partly funded the research activities carried out for this work.

*DOI: http://dx.doi.org/10.5772/intechopen.97809*



## Author details

Vittorio Rosato[1*], Antonio Di Pietro[1], Panayiotis Kotzanikolaou[2], George Stergiopoulos[3] and Giulio Smedile[4]

1 Laboratory for Analysis and Protection of Critical Infrastructures, Enea, Casaccia Research Centre, Rome, Italy

2 Department of Informatics, University of Piraeus, Greece

3 Department of Information and Communication Systems Engineering, University of Aegean, Samos, Greece

4 Degree in Informatics Engineering, Rome Tre University, Rome, Italy

*Address all correspondence to: vittorio.rosato@enea.it

## References

[1] A. Tofani, G. D'Agostino, A. Di Pietro, S. Giovinazzi, M. Pollino, and V. Rosato. Operational resilience: Concepts, design and analysis. *Special Issue "Emerging Approaches to Secure and Protect Critical Infrastructures", MDPI, Submitted*, 09 2020.

[2] A. Tofani, G. D'Agostino, A. Di Pietro, S. Giovinazzi, L. La Porta, G. Parmendola, M. Pollino, and V. Rosato. Modeling resilience in electrical distribution networks. In Samad M.E. Sepasgozar, Faham Tahmasebinia, and Sara Shirowzhan, editors, *Infrastructure Management and Construction*, chapter 3. IntechOpen, Rijeka, 2020.

[3] Alberto Tofani, Gregorio D'Agostino, Antonio Di Pietro, Giacomo Onori, Maurizio Pollino, Silvio Alessandroni, and Vittorio Rosato. Operational resilience metrics for a complex electrical network. In Gregorio D'Agostino and Antonio Scala, editors, *Critical Information Infrastructures Security*, pages 60–71, Cham, 2018. Springer International Publishing.

[4] 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.

[5] Steven M Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, pages 8–pp. IEEE, 2004.

[6] Michel Van Eeten, Albert Nieuwenhuijs, Eric Luiijf, Marieke Klaver, and Edite Cruz. The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Administration, 89(2):381–400, 2011.

[7] Enrico Zio and Giovanni Sansavini. Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Transactions on Reliability, 60(1):94–101, 2011.

[8] J Talsma, B Becker, Quanduo Gao, and ERIK Ruijgh. Coupling of multiple channel flow models with openmi. In *Proceedings of the Tenth International Conference on Hydroinformatics*, 2012.

[9] Serge P Hoogendoorn and Piet HL Bovy. State-of-the-art of vehicular traffic flow modelling. *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering*, 215(4):283–303, 2001.

[10] Samitha Samaranayake, Sébastien Blandin, and Alexandre Bayen. Learning the dependency structure of highway networks for traffic forecast. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pages 5983–5988. IEEE, 2011.

[11] Mohammad Shahraeini and Panayiotis Kotzanikolaou. A dependency analysis model for resilient wide area measurement systems in smart grid. IEEE Journal on Selected Areas in Communications, 38(1):156–168, 2019.

[12] Min Ouyang and Leonardo Dueñas-Osorio. An approach to design interface topologies across interdependent urban infrastructure systems. Reliability Engineering & System Safety, 96(11): 1462–1473, 2011.

[13] Erich Rome, Sandro Bologna, Erol Gelenbe, Eric Luiijf, and Vincenzo Masucci. Diesis: an interoperable european federated simulation network for critical infrastructures. In *Proceedings of the 2009 SISO European Simulation Interoperability Workshop*, pages 139–146, 2009.

[14] Christos Siaterlis, Bela Genge, and Marc Hohenadel. Epic: a testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing, 1(2):319–330, 2013.

[15] George Stergiopoulos, Panayiotis Kotzanikolaou, Marianthi Theocharidou, Georgia Lykou, and Dimitris Gritzalis. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. International Journal of Critical Infrastructure Protection, 12:46–60, 2016.

[16] George Stergiopoulos, Panayiotis Kotzanikolaou, Marianthi Theocharidou, and Dimitris Gritzalis. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. International Journal of Critical Infrastructure Protection, 10: 34–44, 2015.

[17] Adam Hahn and Manimaran Govindarasu. Smart grid cybersecurity exposure analysis and evalution framework. In *IEEE PES General Meeting*, pages 1–6. IEEE, 2010.

[18] Sumeet Jauhar, Binbin Chen, William G Temple, Xinshu Dong, Zbigniew Kalbarczyk, William H Sanders, and David M Nicol. Model-based cybersecurity assessment with nescor smart grid failure scenarios. In *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*, pages 319–324. IEEE, 2015.

[19] Earl E Lee II, John E Mitchell, and William A Wallace. Restoration of services in interdependent infrastructure systems: A network flows approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 37(6):1303–1317, 2007.

[20] Nils K Svendsen and Stephen D Wolthusen. Analysis and statistical properties of critical infrastructure interdependency multiflow models. In *2007 IEEE SMC Information Assurance and Security Workshop*, pages 247–254. IEEE, 2007.

[21] Vittorio Rosato, Limor Issacharoff, Fabio Tiriticco, Sandro Meloni, S Porcellinis, and Roberto Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1-2):63–79, 2008.

[22] White House. *Critical infrastructure security and resilience*. White House, 2013.

[23] Panayiotis Kotzanikolaou, Marianthi Theoharidou, and Dimitris Gritzalis. Assessing n-order dependencies between critical infrastructures. *International Journal of Critical Infrastructures 6*, 9(1-2):93–110, 2013.

[24] Panayiotis Kotzanikolaou, Marianthi Theoharidou, and Dimitris Gritzalis. Cascading effects of common-cause failures in critical infrastructures. In *International Conference on Critical Infrastructure Protection*, pages 171–182. Springer, 2013.

[25] Panayiotis Kotzanikolaou, Marianthi Theoharidou, and Dimitris Gritzalis. Interdependencies between critical infrastructures: Analyzing the risk of cascading effects. In *International Workshop on Critical Information Infrastructures Security*, pages 104–115. Springer, 2011.

[26] T. Macaulay. *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*. Taylor & Francis, 2008.

[27] Alexander Fekete. Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science*, 2:15–24, 03 2011.