Doctorate in Computer Science and Automation

Department of Engineering

XXXI Ph.D Cycle

Modelling Risk in Highly Interdependent Systems

Ph.D Student Cosimo Palazzo

.....

Supervisor Prof. Stefano Panzieri

.....

Ph.D Coordinator Prof. Stefano Panzieri

.....

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than (33669) words including appendices, bibliography, footnotes, tables and equations and has fewer than (65) figures.

Cosimo Palazzo

March 2019

Abstract

Understanding Risk represents the first step in the development of preparedness, resilience and mitigation strategies for governmental and non-governmental organisations. Building a common basis, in such a multidisciplinary context, becomes more and more a necessity because it helps us focus on the true nature of risk and not only on individual or circumstantial aspects which compose it. Starting from this perspective it is mandatory to continuously improve risk approaches and methodologies in our modern and fast changing society.

The aim of this work is to provide a new Risk Analysis terminology-based framework and then introduce the MHR-RFB approach (Mixed Holistic Reductionist - Rational Fuzzy Bayesian) to model complex scenarios in highly interdependent systems. Subsequently an agent-based simulation software (CISIApro) is presented as a tool capable of implementing the MHR-RBF approach and promote a new Dynamic Risk Analysis (DRA).

Thanks to the DRA it is possible to create a new generation of on-line tools able to dynamically assess the risk and supply an effective Decision Support System (DSS). In the second part of this work are proposed some applications of these strategies, in different critical contexts, to demonstrate how it is possible to convert risk data in a powerful source of information and use it to protect our contemporary society.

Table of contents

List of figures

List of tables

Chapter 1

Understanding Risk

The deeper we get into Risk Analysis issues, the more we begin to understand that a lot of terminology inaccuracies are commonly adopted. In meetings where people have heterogeneous backgrounds, it can happen to discuss for hours about risk methodologies mistakenly adopting common definitions without realising it. Since it may lead to confusion it is a mandatory step to build a common terminology basis before approaching topics related Risk Analysis.

Several agencies and national bodies have perceived the same need, as well as UNISDR (The United Nation Office for Disaster Risk Reduction) that starting from July 2002 (and then in 2004, 2005 and 2009 [2]) has proposed a set of basic terms used for the Disaster Risk Reduction. Subsequently, in August 2015, the same agency, has supervised a technical review in order to update such terminology [3]. This attention attests the high topic sensitivity showing just how it is important to define a common vocabulary.

Risk scenarios are so complex and composed of various facets that is very difficult to provide a comprehensive model for all of them in a unique 'final truth'. Risk evolves as fast as modern society and its public perceptions, that are product of economic interests, reflect a specific cultural heritage often linked to the territory. Sometimes disagreement

and mistrust lead to better ideas but to prevent debates, which could exacerbate divergences and compromise risk management strategies and decision processes, it is important to understand inherent nature of the risk and how it evolves over time.

The main aim of this section is to take a step back examining the meaning behind the most popular terms used in the risk analysis discipline, sometimes even stressing their definitions. Its ambition is to provide a valid contribution in shaping a useful practice for risk experts, especially when dealing with highly interdependent systems.

Not carrying out this step would mean not to clearly define the meaning and the scope of proposed methodologies and tools.

1.1 Risk

It is interesting to see how risk perception has always been part of people's life and how it has been historically interpreted. The Oxford English Dictionary cites the earliest use of the word in English (from French 'risque' danger or inconvenience, predictable or otherwise) as of 1578 in Middle French as a feminine noun, in 1633 as a masculine noun, in 1690 as a legal term and spelled as risk from 1655. It defines risk as:

> ***Risk*** *– (Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility.*
>
> [The Oxford English Dictionary]

In this first definition we can see how the '*Risk*' was perceived as an '*exposure*' to possible loss or damages in unpredictable circumstances. As we will see this perception will evolve into something more complex and punctually identifiable.

It is undisputed that there is no agreement on final definition of Risk. This is because when we speak about Risk is important to consider the social contexts in which risk arises and the perception of risk by the involved '*actors*'. As pointed out in Terje (2009) [4], Risk term can be divided into two main categories:

1) Risk expressed as probabilities and expected values

- Risk equals the expected loss [5];
- Risk equals the expected disutility [6];
- Risk is the probability of an adverse outcome [7];
- Risk is a measure of the probability and severity of adverse effects [8];
- risk is the combination of probability of an event and its consequences [9];

2) Risk expressed as events, consequences and uncertainties

- Risk is defined as a set of scenarios s_i, each of which has probability p_i and a consequence c_i [10];
- Risk is equal to the two-dimensional combination of events/consequences and associated uncertainties (will the events occur, what will be the consequences) [11];
- Risk refers to uncertainty of outcome, of actions and events [12];
- Risk is a situation or event where something of human value (including human themselves) is at stake and where the outcome is uncertain [13];
- Risk is an uncertain consequence of an event or an activity with respect to something that humans value [14].

One of the most recognised definition of risk can be taken by **ISO 31000:2009** [15]. The main scope of *ISO 31000* is to provides principles and generic guidelines on risk management. Such international standard is associated with a new definitions vocabulary *ISO Guide 73:2009* [16].

> ***Risk*** *– is the effect of uncertainty on objectives.*
>
> [ISO/FDIS 31000:2009(E)]

Following Risk definition, five note are underlined:

1. An effect is a deviation from the expected - positive and/or negative;
2. Objective can have different aspects and can apply at different levels;
3. Risk is often characterized by reference to potential events and consequences, or a combination of these;
4. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood;

5. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

[ISO Guide 73:2009]

All Risk definitions in literature can co-exist because while *ISO 31000* define risk from a generic point of view, in *goal-oriented* terms, other definitions are usually defined in *event-oriented* terms.

Please note that the English term *Likelihood*, as mentioned in ISO Guide 73:2009, is used to refer to "*the chance of something happening*" and does not have a direct equivalent in some languages, resulting maybe misleading for not English native speaking. The term **likelihood** *provides a guess at the odds of something happening not backed up by quantifiable facts* as opposed to Probability that is often expressed as "*measure of the likelihood an event will occur*" ([17]). Indeed, Mathematical meaning of *Probability* and *Likelihood* are different starting with the fact that *Probability* is a 'quantifiable' measure. For this reason, definitions, often found in literature (i.e. SRA Glossary), which pose an equivalence between these term can be reviewed in this optic.

Approaching the meaning of 'likelihood' to the concept of "*the* ***possibility*** *of something may happen*" enables to introduce different mathematical frameworks with respect to common probability use.

For instance, introducing Fuzzy Theory as proposed in [18], to model humans granulate information and reason, allows introduction of set-theoretic deduction mechanisms, through domain experts interviews, bypassing problems inherent to reach historical data on new or less known assets. But this could be just one of many mathematical techniques which could be used to overcame the limitations linked to consistency of produced risk-oriented data.

Concluding, *Likelihood*, could also be expressed as an inexact, qualitative statement of how one assesses probability.

Likekihood *– represents the possibility that a given event will occur.*

Likelihood could be also expressed as an inexact, qualitative statement of how one assesses probability.

Due to the numerous definitions, that it is possible to find in literature, it is easy to get confused and think that a Risk Index is a numerical probability or that it is plausible to apply the mathematical framework of the well-known statistical analysis to it. Therefore it is necessary to clarify that, although some of these concepts might be used to comprehend the meaning of this value, **Risk is not a mathematical probability** but a metric, an index with a high information content, able to get a '*sensitivity*' or a '*measure*' of how we are exposed to certain evens occurrence and what might be their impact and consequences. It is a common practice to define a measure of Risk as:

$$Risk \;=\; Probability\,(of\ Occurrence) \;\times\; Impact\,(of\ Risk)$$

This formula suggests a functional relationship between *Risk Occurrence* and its presumable *Impact* but it has not a solid mathematical foundation since it brakes *Probability Theory* and inductive logic axioms (in other words, it makes no sense!). It would be more appropriate to rewrite the formula as a generic function of its main terms, $R = f\,(P,\ I)$, simply stating a correlation between *Risk Probability* and *Impact*. This correlation can be then differently formalised based on specific methodologies. An example of that is the **P-I Table** framework which offers a classification for risk ranking. With the P-I Table a *Risk Score* matrix is built where higher values are associated to greater levels of risk. Following this technique, the **Severity** term is defined considering a single type of impact:

$$Severity \;=\; Probability \;+\; Impact.$$

Severity scores are then used to determine the most important risks, enabling management bodies to focus resources consistently in order to reduce or eliminate them. This shows that it is more effective to use risk expression $R = P \times I$ as a starting point towards building a risk methodology rather then strictly applying it.

In February 2007, CRS (Congress Research Service) released the report RL33858 [19], "*The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*". As we know, DHS represents one of the most important reference in the Risk Analysis field due to the sensibility and investments of USA government about Risk Terrorist Attack prevention and mitigation. This report presents the evolution of Risk Assessment Methodologies tracking major milestone events in USA Homeland Security contexts and Fiscal Years (FY).

---

*A **Fiscal Year** (FY) is a period that a company or government uses for accounting purposes and preparing financial statements. A fiscal year may not be the same as a calendar year, and for tax purposes, the Internal Revenue Service (IRS) allows companies to be either calendar-year taxpayers or fiscal-year taxpayers.*

[FY Definition | Investopedia.com]

Risk formulas, evolution and ramifications, are utilised to allocate homeland security grant founds. Three main stages have been identified [19]:

Stage I - from FY2001 to FY2003

The *Department of Justice* (DOJ) and *Department of Homeland Security* (DHS) where respectively responsible for risk assessment guidelines definitions during FY2001 and from FY2002 to FY2003.

$$\mathbf{R}isk \;=\; \mathbf{P}opulation$$

Stage II - FROM FY2004 TO FY2005

In this period risk as probability was not considered in Risk Assessment process. On the other hand Population Density, Critical Infrastructure and Threat were included using the additive formula bellow:

$$\mathbf{R}isk \;=\; \mathbf{T}hreat + \mathbf{C}ritical\ \mathbf{I}nfrastructure \;+ \mathbf{P}opulation\ \mathbf{D}ensity$$

Stage III - FROM FY2006 TO TODAY

Probability was introduced and for the first time DHS risk assessment was focused on both assets and geographic areas. Risk expression have sustained some important considerations turning it into the well-known formula which takes into account *Threat* to a target/area, multiplied by *Vulnerability* of the target/area, multiplied by *Consequence* of an attack on that target/area.

$$\mathbf{R}isk \;=\; \mathbf{T}hreat \times \mathbf{V}ulnerability \;\times \mathbf{C}onsequence$$

Taking decision with this formula means, for instance:

- **Risk can either be accepted or ignored**: in all those situations where *Consequences* are insignificant, even when Threat and Vulnerabilities are high (i.e. adequate levels of protection are not reached);

- **Mitigation or Reaction strategies are adopted**: for instance, in case of significant Vulnerabilities, which could be triggered by a high level of Threat, in a situation where possible consequences are severe.

As regards the associated formula weight, in FY2007 DHS specify elements and sub-elements as follows:

- Threat Index [20%]
- Vulnerability & Consequence [80%]
  - Population Index [40%]
  - National Infrastructure Index [15%]
  - Economic Index [20%]
  - National Security Index [5%]

To avoid further confusion it is important to understand that the DHS's Risk Formula, with its assigned weights, is also used to distribute funds to USA state and local communities. Although it is important to be focused on the government's risk perceptions and its priorities, design efficient solutions to prevent and mitigate risks, is a totally different process. In fact, the International Standard Organisation itself, in the ISO 31000:2009, claims that it does not have the intent to promote a unique Risk framework, across different organisations; it recommends instead to approach risk management and its application taking into account the specific needs of each organisation, its objectives, context, structure, operations, processes, functions, projects, products, services, assets and so on. That is to say, that it is mandatory to correctly interpret, in a certain context, the DHS's Risk Formula without blindly applying it to different contexts. Strictly using Risk formula may limit the perception of risk in some critical situations in which risk analysis involves highly interdependent systems affected by possible cascading effects. Due to the different needs in such a multidisciplinary area, after this risk formula, a considerable number of variations and interpretations were proposed but they all revolve around the same concepts.

The following sections identify and define the main steps proposed in this approach, explaining the meaning of the involved risk terms and collocating them in an iterative dynamic process (Fig. 1.3). Such a logical process, due to its iterative nature, is particularly suitable in highly interdependent contexts where an appreciable number of (inter)dependencies can model a really complex reality difficult to analyse with common risk frameworks.

1.2 Asset [Identification]

When we start with any Risk Analysis approach, it is unquestionable that, the first problem concerns the capability to understand what the most '*sensible*' aspects of an organisation are. This not only means to consider all the '*tangible*' aspects of an organisation but, in the same way, to take into account aspects like knowledge, know-how, intellectual property, brand, political clout and all its intangible assets. Hence, intangible assets exist in opposition to tangible ones which represent strategical non-physical characteristics of an analysed organisation.

Typically an organisation distinguish short-term assets from long-term resources. Being the first type linked to a short-term financial concept (1 year) the long one are the most significant for the stability and continuity of an organisation. Borrowing a good asset definition, it can be said that:

> ***Asset*** *– People, property, and information. People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.*
>
> [WWW.THREATANALYSIS.COM]

Asset Identification phase could be a high sensible step due to a possible wrong coarse level of granularity assigned to a specific analysed asset. Consequently, such a wrong practice might causes inappropriate risk identification associated to particular elements.

Because of their nature, in most cases, assets are mutually interdependent due to their proximity and their interactions. Therefore, it is crucial understand what are the assets which can trigger dangerous domino effects in a highly interdependent context. Correctly identify this aspect it is what that could differentiate a proper analysis process from a wrong one.

Using a criteria which takes into account combination of asset health and criticality could help Risk Management to prioritise and define specific risk assessment process as outlined in Transpower Criticality Framework (2013).

1.3 Hazards [Analysis]

Once that tangible and intangible assets, of an organisation, are identified it is possible to proceed to a *Hazards Analysis* process considering possible losses or damages. In the *Risk Assessment* context an hazard is defined as:

> ***Hazard*** *– A potential damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic distruption or environmental degradation.*
>
> [UNISDR 2004]

in other words:

> ***Hazard*** *– Is the source of a danger which can cause an asset loss or destruction.*

Common *Hazards* are usually grouped by Natural, Social, Organizational, Thecnological and Behavioral hazards [20] such as:

- Fires [Natural]
- Floods [Natural]
- Earthquakes [Natural]
- Tornados [Natural]
- Tsunamis [Natural]
- Lightning [Natural]
- War [Social]
- Sabotage [Social]
- Terrorism [Social]
- Communicable disease [Social]
- National security hazards [Social]
- Long working hours [Organizational]
- Inadequate competence[Organizational]
- Dam failures [Technological]
- Hazardous materials [Technological]
- Nuclear accidents [Technological]
- Power failures [Technological]
- TELCO failures [Technological]
- Gas & Oil distr. failures [Technological]
- Water distr. failures [Technological]
- Transportations block [Technological]
- Industrial accidents [Technological]
- Bad habits [Behavioural]
- Drug and alcohol abuse [Behavioural]
- Environmental changes [Behavioural]

An *Hazard* of natural or human origin, incorporating latent conditions, can turn into future *Threat*. It represents, not a specific event but, a **prerequisite for the occurrence of a dangerous situation**. Another important point, concerning the *Hazards Analysis*, is to consider not only the actual condition of an asset but all its different life stages such as: Maintenance, Decommissioning and so on. In conclusion, the main objective of a *Hazards Analysis* process is to identify all potential hazards into the considered environment starting from a coherent *Assets Identification*.

1.4 Threat & Threat Actor [Analysis/Identification]

Occasionally, terms *Hazard* and *Threat* are overlapped but it must be made a substantial differentiation between them:

*While **Hazard** represent the possible risk source (origin of danger), **Threat** expresses what which triggers **Vulnerability**.*

It should be noted that where there is an *Hazard* we may or may not be *vulnerable* to it. For example, people contract BCE - Bovine Spongiform Encephalopathy (*Hazard*):

- You have a meaty diet THEN you are *vulnerable* to BCE;
- You are vegan THEN you are *not-vulnerable* to BCE.

Generally we can find the word **Threat** defined as:

Threat *– The likelihood of an attack occurring.*

[CRS RL33858]

Threat *– Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.*

[WWW.THREATANALYSIS.COM]

In some cases, reference is made to the dependency of two factors, '*Intent*' and '*capability*'. The function:

$$f(Intent \times Capability)$$

refers to the enemy's capability and intent to conduct attacks on a well-defined target/area. To develop a heightened sensitivity to the *Threat* term, from the point of view of its intentionally or unintentionally, a more complete definition could be:

Threat *– Is a negative event which can cause an undesired or unexpected outcome, such as damage to, or loss of, an asset. It can become more dangerous due to a system vulnerability, use a vulnerability into a system or create new vulnerabilities in one or more interconnected systems.*

in other words:

Threat *– Is anything that might exploit a vulnerability.*

Usually, the term *Threat* is indistinctly used to indicate both *Attack* and *Threat Actor*, and often to define a *Danger*. Some examples of Threats are:

- A fire *starts* in a near forest [Geographical];
- A flood *affects* your headquarters [Geographical];
- An operator *accidentally* turn off a SCADA component [Physical];
- A Terrorist *begins* to buy suspicious material to create a bomb [Physical]
- A Cybercriminal *undertake initiatives* in order to steal sensitive data [Cyber];
- A foreign government *attempt* to compromise national cyberspace [Cyber];
- An employee *try* to sell organization secrets to a prowler [Logical].

Defining a *Threat* consequently helps in identifying the *Threat Actor*:

Threat Actor *– Is a person, entity, natural event or organization which could be leading case of the given scenario.*

Obviously, the definition makes more sense when we refer to human-driven scenarios rather then natural disasters like flood, fire or earthquake. Also *Threat Actors*, as well as the nature of a threat, can be divided into two different categories: intentionally and unintentionally.

Common ***Threat Actors*** could be:

- Terrorists;
- Hacktivists;
- Cybercriminals;
- Business-oriented attackers;
- Casual attackers;
- Unreliable insider;

- Corrupted people;
- Malicious (generally);
- Careless operators;
- Governments/Nation States;
- Nature;
- Unpredictable actors (Alien invasion!).

1.5 Vulnerability [Assessment]

Even for this term, there are a certain number of interpretations available in literature. This is because such word refers, sometimes, to 'possible' exploitable *Threat* or to 'well-known' *Assets* weaknesses. In this same vein, we notice that there could be 'chronological' identification issues (with reference to past, future or present) to correctly assess vulnerability. Often, to such term, are associated conditions determined by physical, economical, social and environmental factors. Due to the difficulties to identify vulnerability measures, across different areas, in some reading, we find *Vulnerability* and *Consequence* evaluated as single variable (V&C). Another confusion usually arises over *Vulnerability* and *Exposure*. In the Exposure paragraph we will try to clarify this aspect. Following some commonly agreed definitions of *Vulnerability*:

> *1)* ***Vulnerability*** *– Any weakness in an asset's or infrastructure's design, implementation, or operation that can be exploited by an adversary. Such weaknesses can occur in building characteristics, equipment properties, personnel behaviour, locations of people, equipment and buildings, or operational and personnel practices.*
>
> [RAMCAP^{TM} Framework 2006]

> *2)* ***Vulnerability*** *– The conditions determined by physical, social, economical factor or process, which increase the susceptibility of a community to the impact of hazards*
>
> [UNISDR 2009]

3) ***Vulnerability*** *– The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.*

[ITSEC]

All three examples have some limitations in their interpretations. Although the first one is a good definition, linking *Vulnerability* only to intentionally of an attacker could be a misleading understatement while the second definition sounds synthetic and unclear. The last one, instead, is restricted to the IT context. Taking into account already defined terms (and other ones that we will define later) we can state that:

Vulnerability *– Is a latent weakness of an asset (or a group of assets), that can be exploited by one or more "Threat Actors", increasing sensitivity to the "Consequence" of "Hazards". The weaknesses may be physical, technical, operational, and organizational*

Vulnerability Analysis and *Assessment* disciplines represent a fundamental part of Risk Management because they offer a comprehensive overview about the actual scenario. They are also good indicators which express *how well we are managing risks*. Basically we take what was identified during information gathering and determine the current exposure of our systems to specific vulnerabilities.

Assess vulnerabilities requires an extensive sectorial/domain knowledge and expertise, across different context in order to deeply understand how components, factors and processes may interact with each other producing complex cascading effects. Many of these vulnerabilities are the result of inefficient security governance, wrong strategies or inadequate architectures. Below, some example of *Vulnerabilities*:

- A weakness in a firewall;
- Bad maintenance management;
- Lack of security;
- Sensors or actuators faults;
- Inadequate architecture;
- Clumsy operators;

- Inadequate personnel;
- Approximative system design;
- Security policies;
- Wrong procedures;
- Remote access;
- Hazardous materials;
- Geographical location;
- Old structures.

1.6 Impact & Consequences [Assessment]

It was chosen to group this two terms in a single paragraph because *Impact* and *Consequence*, fundamentally, express the same concept. Starting from the analysis of 'consistent' historical data, impact assessment criteria may include all the consequences with respect to assets and people regarding: physical, financial, reputation, regulatory and environmental conditions. The well-known risk formula is an example considering the wide variety of its versions where both terminologies are indistinctly adopted.

Reading *ISO 31000:2009* [15] guidelines, we simply define *Consequence* as:

> ***Consequence*** – *Outcome of an event affecting objectives.*
>
> [ISO/FDIS 31000:2009(E)]

where '**Event**' means "*occurrence or change of a particular set of circumstances*". Then, in ISO Guide 73:2009 [16], four note are underlined:

1. An event can lead to a range of consequence;
2. A consequence can be certain or uncertain and can have positive or negative effects on objectives;
3. Consequences can be expressed qualitatively or quantitatively;
4. Initial consequences can escalate through knock-on effects.

[ISO Guide 73:2009]

Other interesting definition are provided by the RAMPCAP framework:

> ***Consequence*** *– The outcome of an event occurrence, including immediate, short- and long-term, direct and indirect losses and effects. Loss may include human casualties, monetary and economic damages, and environmental impact, and may also include less tangible and therefore less quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness, or other impacts.*
>
> [RAMCAP™ Framework 2006]

An *Impact Assessment* process is a methodology used to determine probabilities or estimate the consequences magnitude of an event outcome. The results of such process are then used to prioritise decisions and managing criticality. Potential damages caused by some specific events may have dimensions and repercussions at different levels. For this reasons it could be useful to make a little differentiation between *Impact* and *Consequence* 'stressing' their concepts.

For instance, considering an organisation composed by several departments (Fig. 1.1), when a strategical sector is affected by a loss, we could say that:

– There is an *Impact* in the strategic sector;

– There will be *Consequences* for the organisation.

We have two different aspects to consider. The first one is strictly correlated to the possible damages timing because *Impact* may cause '*abrupt*' losses, while, when we analyse possible *Consequences* we deal with '*incipient*' losses with effect on several 'dimensions'. In fact, while in an *Impact* we look at a *punctual* asset loss (strategical sector), with *Consequences* we take into account repercussions at the Organisation level.

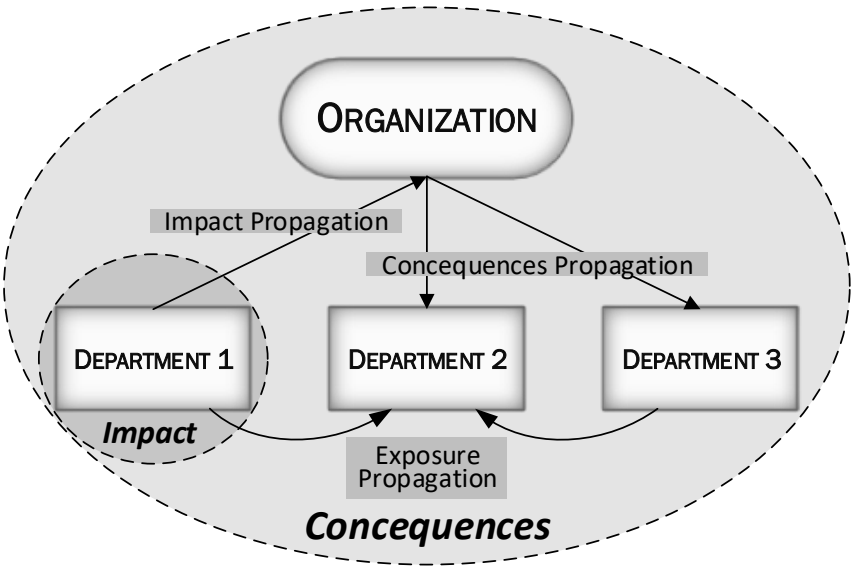


Figure 1.1 Impact vs Consequences vs Exposure propagation.

1.7 Exposure [Assessment]

Frequently, *Exposure* with *Vulnerability* or *Exposure* with *Consequence* are confused and sometime used as synonyms. It should be noted that there is a slight difference between those terms.

In accordance with "*Exposure and Vulnerability UNISDR Working Group* short note" [21] it is important to understand conceptual differences between this two terminologies in order to improve our comprehension about risk nature. Some *Exposure* definition are:

> ***Exposure*** *– The people, property, systems, or other elements present in hazard zones that are thereby subject to potential losses.*
>
> [UNISDR 2009]

> ***Exposure*** *– The potential loss to an area due to occurrence of an adverse event.*
>
> [ISACA]

Both definition are, markedly, characterised by a 'physical' proximity concept. Although this is correct, it could be limiting when we refer to an economical, social, organisational, logical or cyber fault propagation of risk. For instance, such definitions, would not be valid if we say:

- A computer network security *vulnerability* could *expose* the bank to economical losses [from cyber to economical];
- A control fault (*vulnerability*) in the SCADA could *expose* our system to cyber attacks [from logical to cyber];
- High tax burdens in a financially unstable company (*vulnerability*) would *expose* it to a possible bankruptcy [from socio-political to economical].

Referring to an hypothetical interdependencies model, we can easily understand how the *cascading effects*, due to events propagation, involves 'near entities' to particular *risk exposure* conditions. Moreover, linking different 'domains' makes it possible to spread new *vulnerabilities* towards specific *assets* and consequently *expose* them to future losses. Hence, we can define *exposure* as:

Exposure *– Is a condition that could cause future loss (or losses) which are the result of activity, occurrence or their propagation.*

1.8 Summary

We have gone through the common terminology used in Risk Analysis and Assessment frameworks, trying to clarify, and where possible differentiate, interpretations by the adoption of specific terms. This is not intended to be a purely formal exercise but to help punctually recognise different aspect of *Risk*. Making this initial effort facilitate the production of consistent risk models (as accurate reflections of reality) and appropriate decisions making systems capable to reduce or mitigate risks in specific critical situations.

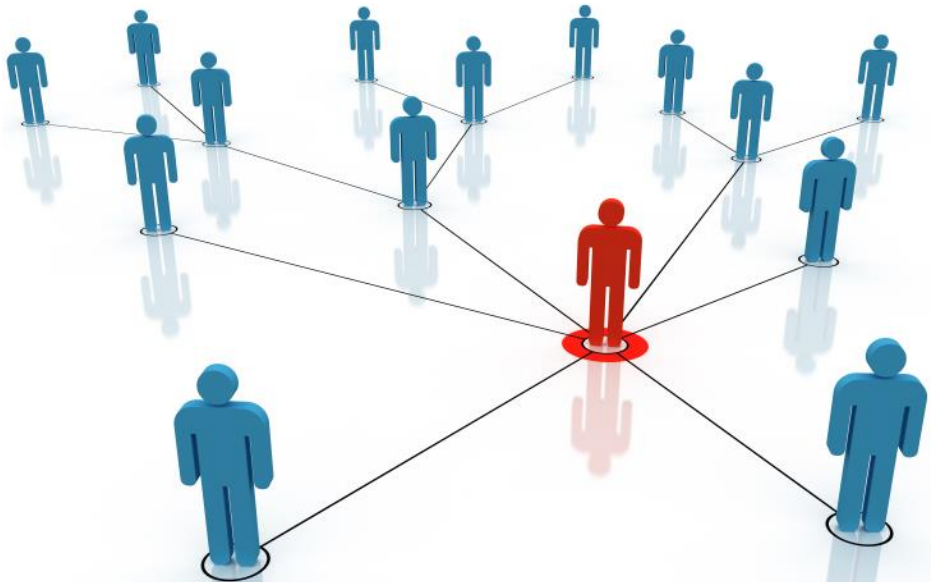


Figure 1.2 Spreading infection: a risk example.

In order to logically collocate all terms used so far, it is possible to propose, as a mental exercise, an out of context example. Imaging to stay within a crowded public place, analysing a simple situation like a common cold diffusion, we may say that:

- ***Scenario***: A crowded public place;
- ***Exposure*** (*suffered*): Being in a public place;
- ***Asset***: Our body;
- ***Hazard***: The common cold;
- ***Threat***: Sneezing of a cooled person;
- ***Threat Actor***: The cooled person;
- ***Vulnerability***: Low immune defences;
- ***Impact***: Physical problem caused by the infection;
- ***Consequence***: Propagation to a higher (*social*) dimension;
- ***Exposure*** (*induced*): Spreading infection to nearby people.

The example above also emphasises a dual nature which can be assigned to '*Exposure*' interpretations in a given scenario. It is directly connected to complex and highly interdependent systems. Therefore, if the 'current' analysed asset suffers an exposition, due to a previous malicious propagation, it is a different condition than an induced exposure due to being the main propagation cause.

Considering now a highly interdependent context in which risk propagation spans different organisational layers we can identify two kind of situations (see Fig. 1.1):

- **Horizontal propagation**: risk exposure propagation occurs between punctually identified assets (more related to a reductionist representation);

- **Vertical propagation**: occurs when a risk impact propagation evolves in risk consequences at a global level (spreading from a reductionist dimension to a more holistic point of view).

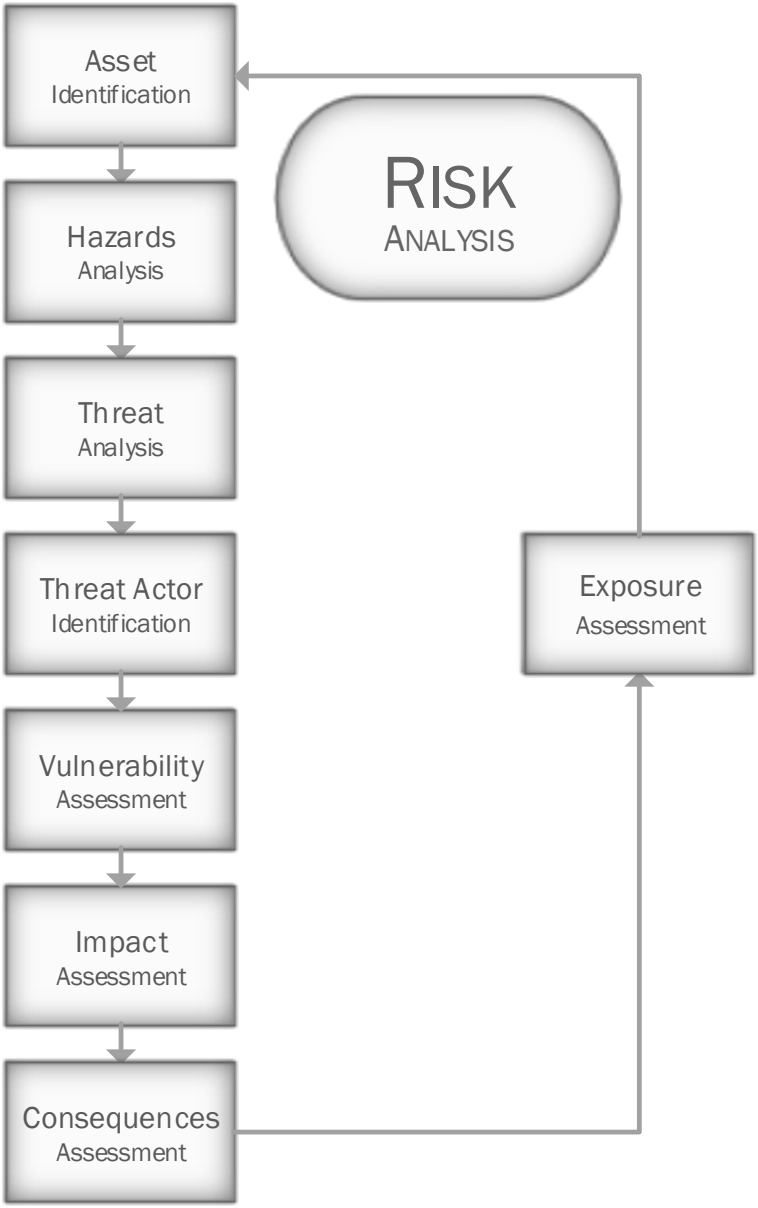


Figure 1.3 A Risk Analysis process.

1.9 Chapter Conclusions

Proposed Risk Assessment framework is nothing more than a simplified process where it is essential deeply understand well-known risk terminology. Adopting the proposed sequential logic schema (see Fig. 1.3) shall make available an iterative methodology able to assess the risk through an ordered sequence of steps which consider also strategical assets proximity. Furthermore, allowing an integration of cascading effect mechanisms and propagation simulation engines we can create efficient online tools able to asses a dynamic risk evaluation in complex highly interdependent scenarios.

Although, classic risk techniques are an important plank for our society these considerations mean that the continuous improvements of emerging technologies (i.e. 5G architectures) increasing their complexity, push towards including a new kind of Informed Dynamic Risk Assessment (IDRA) in parallel with classic Risk Assessment and Management approach. Adopt an online IDRA systems is mandatory in order to maintain high level of Business Continuity (BC), unexpected events preparedness and Quality of provided Services (QoS) considering that a risk measure may change over time and is conditioned by the state of 'influencer' assets proximity.

The aim of this chapter is to provide a common terminology basis clarifying the fundamental principles of such a discipline. Although it might seem redundant, it gives us the opportunity to have a unique 'universal language' in multi-domain contexts. There are a number of techniques used to identify, assess and manage the risks. This part of the Risk Analysis continuously promotes a constructive discussion around the most sensitive areas of governmental and non-governmental organisations. It represents the first element of a chain which has as its main aim the protection of strategical assets of an organisation together with the safeguarding of provided services, their sustainability and continuity over time.

Chapter 2

Mixed Holistic Reductionistic - Rational Fuzzy Bayesian (MHR-RFB)

Adopting a Mixed Holistic Reductionist approach means have a methodology able to provides a defined set of tools for modelling the real complexity in highly interdependent systems compared to a required abstraction level and the available information. To complete this already effective approach, in this work, are proposed some improvements both for better understand modelled elements and for concomitantly use different mathematical framework at the same time (not mixing them but using them together!). This makes possible exploit data and information of different nature and fuse it in a unique framework producing an Informed Dynamic Risk Analysis (**IDRA**) tool. While the first three letters **MHR** express the capability to model different '*granularities*' (abstraction levels) in a same model, the next three letters **RFB** reveal the possibility to exploit information defined by '*numbers*' of different nature representing different behaviours in a same model. With the MHR-RFB it is proposed a functional approach

oriented to the Risk Assessment discipline with a high informational content both from an academic and didactic perspective.

2.1 Dependencies, Interdependencies and Complex Systems

Considering infrastructures as isolated '*cathedrals in the desert*' is a nasty simplification which does not objectively express hidden nuances of the reality and therefore does not consider complex iterations such as organizational, geographical, virtual, socio-economical, socio-political and so forth. Indeed, not taking into account this 'reality' means not having the capability to 'detect' unpredictable behaviours due to the analysis of a single isolated part of a global framework.

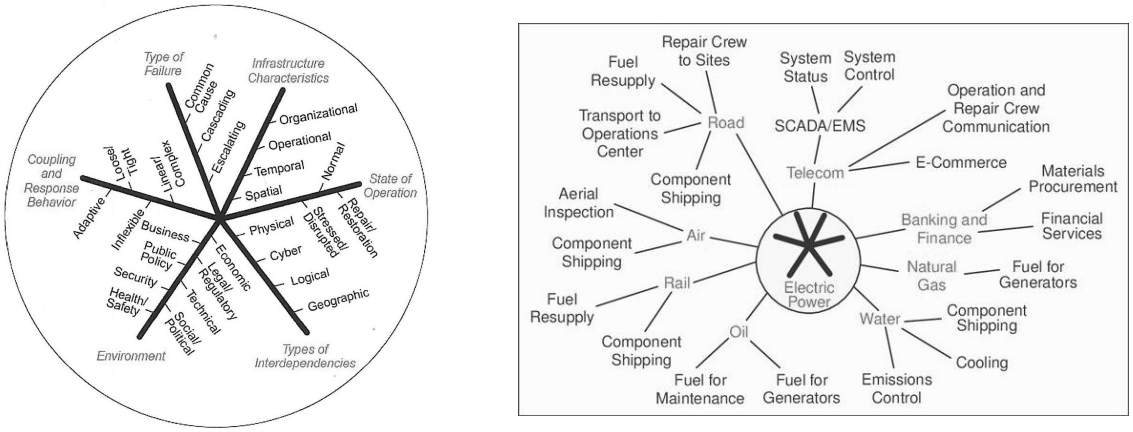
As we can image Infrastructures affects every day our social sphere influencing our perception about quality of life. In this sphere we could consider services like electric, water, gas, telecommunication, transportation, agriculture, financial, economical political, government administrations and all that are part of the national population well-being. In order to express the '*connection degrees*' among infrastructure, CI community started working to understand how the most 'centrics' infrastructures could affect other ones.

Dependency – *Linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.*

[Rinaldi et al., 2001]

Hence, we define a *dependency* as unidirectional relationship between two complex systems in case of a system A directly dependant on system B through a link, but not

the contrary. Although, introducing detailed dependencies improves the comprehension of the reality, unfortunately, is not sufficient.



(a) Dimentions (b) Dependencies

Figure 2.1 Electric Power infrastructure dependencies [Rinaldi et al., 2001].

For instance, consider unidirectional dependency between a power distribution system and a telecommunication network system is a limited outlook if we think about the SCADA systems which nowadays control new generation power grids. For this reasons *interdependencies* was introduced.

> ***Interdependency*** – *A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.*
>
> [Rinaldi et al., 2001]

Hence, we define an *interdependency* as bidirectional relationship between two complex systems in case of a system A directly dependant on a system B through a link and the same system B directly dependant on the system A through other link. Functional dependencies and interdependencies in complex systems are, often, too difficult to describe only in a single scenario, due to the presence of direct and indirect

relations. On the other hands, introduce new correlation with other systems means improve the model and consequently our knowledge about considered scenario.

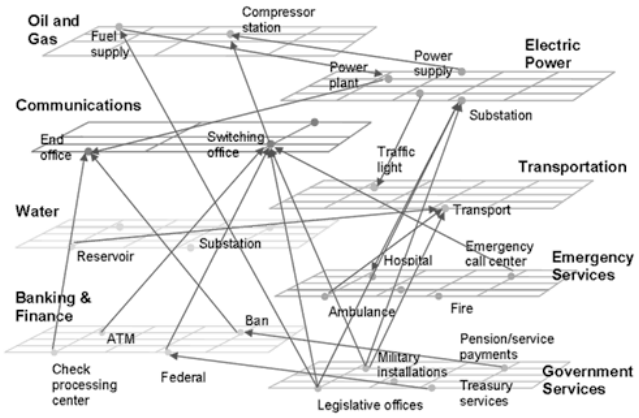


Figure 2.2 Interdependencies example.

We notice that, in complex systems discipline, is mandatory to consider the *time dimension*. This because it is clear how some infrastructure components (physical and not) are strongly influenced by past experience and its performance deterioration in time.

In [22] authors identify four 'main' dependencies which are not mutually exclusive:

– Physical Dependency –Two infrastructures are physically dependent if the operations of one infrastructure depends on the physical output of the other;

– Geographical Dependency –A geographic dependency occurs when elements of multiple infrastructures are in close spatial proximity. In this case, particular events, such as an explosion or a fire in an element of an infrastructure may create a failure in one or more near infrastructures;

– Cyber Dependency –An infrastructure has cyber dependency if its state depends upon information transmitted through the ICT (Information and Communication Technology);

– Logical Dependency –Two infrastructures are logically dependent if their dependency is generated via control, regulatory or other mechanisms that cannot be considered physical, geographical or cyber.

There were numerous further similar proposal who tried to introduce other dependencies levels like Economical, Political, Organizational, Social and so on, but we may consider all of them sub-level of the most generic *Logical Dependencies* level. Anyway, there is no limit in introducing new levels to improve the explanatory capacity in a specific case study model.

2.2 Mixed Holistic Reductionist (MHR) Approach

Thinking the Unthinkable is an euphemism which tells us how it is difficult to take into account a huge amount of information, some time of unknown, hidden or unpredictable element, during the Risk Analysis process. In Critical Infrastructures Protection (CIP) one of the greatest challenge regards the capability to correctly address a functional model able to express, with an acceptable level of abstraction/granularity, the complexity of a defined scenario.

Improve the knowledge about such topics means understand, from different perspective, behaviours, characteristics, dynamics and followed patterns of considered *System of Systems* which are characterized by many *dependencies* and *interdependencies*. The Mixed Holistic Reductionist (MHR) approach, proposed by [23], was created to exploit the advantages of holistic and reductionist methods.

With the **Holistic Framework** all infrastructures are considered as a whole taking into account only High-Level iterations. From the '*holistic*' point of view, infrastructures are seen as singular entities with defined boundaries and functional properties. It is generally simplified, very abstract and strategic oriented. It stems from the need to have a good representation reducing the most common issues posed by the fact that in

CI are highly sensitive and most of the informations are not publicly available (*Sharing Information Problem*) for the national security.

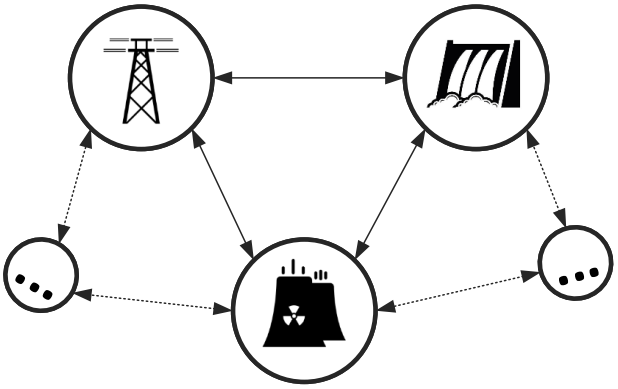


Figure 2.3 Holistic Approach representation.

In this way each infrastructure is modelled as an atomic entity with a Higl-Level of approximation empathizing the role played by each of them into a global scenario. Hence, the **level of operability** of considered infrastructures directly depends on the availability of **resources** supplied by other CIs. On the contrary, a **fault** propagation (cascading effect) may introduce performance degradation by creating negative chain events. Commonly, an holistic model, is treated as a qualitative technique included into the *Global Analysis*. Needed information usually came from linguistic field collected via round table, stakeholders, domain experts interviews, questioners and so on.

In conclusion, such methodology, is very attractive because allow a *Macro-Scale* consequences analysis among expert of different areas using a simple, familiar, framework.

Reductionist modelling accentuates the need to fully comprehend roles and behaviours of individual components to truly understand the infrastructure as a whole. Reducing a situation/scenario into its component elements means manage outcome archiving a desired level of knowledge. From this perspective a situation consists of a

sum of its *micro-scale* components parts in order to '*reduce*' and separately analyse each fragmentation of these. If a greater detail is required then it will be necessary to progressively reduce component into smaller sub-components. This reiterative process can stops only when the expected detail level and understanding were reached.

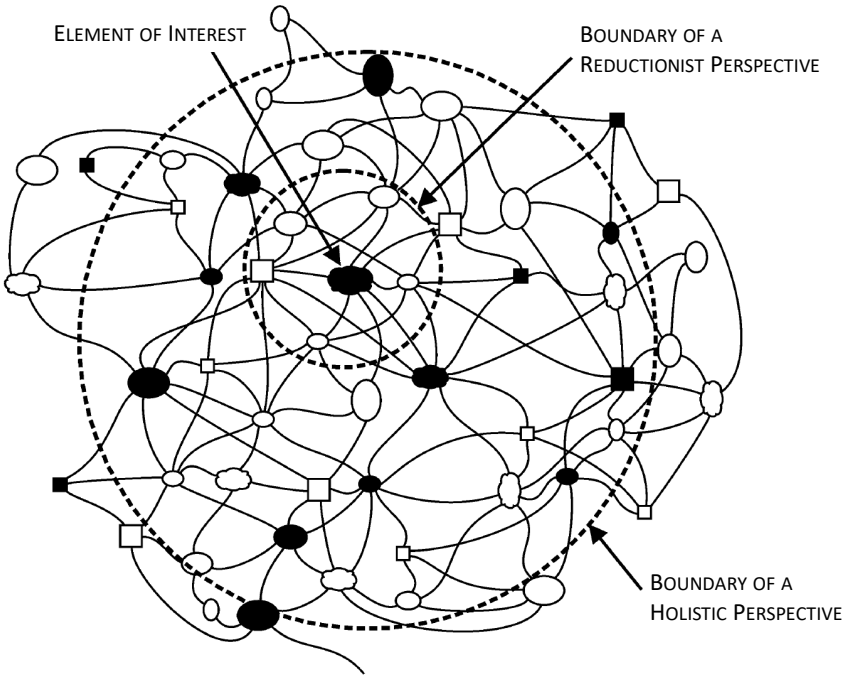


Figure 2.4 Holistic vs Reductionist perspective [1].

Different levels of analysis require one or both of the two proposed point of view and their boundaries are lost in event of complex case studies. In according with [24], dealing with complex highly interdependent scenarios, one of the biggest mistake could be analysing them using a single perspective stressing or reducing concepts and knowledge with regard to the effectiveness of the representation. In addition, in the same work, are presented three hierarchical levels:

– Micro-Level –represents the physical components that constitute the functional elements of an infrastructures (i.e., electrical equipments, gas valves, etc.);

- Meso-Level –represents an infrastructure network at the system level (i.e., network nodes and links, power generators and loads, etc.);
- Macro-Level –represents the territory or zone which depend on the service provide by the infrastructure.

As we have seen *Holistic* and *Reductionist* approaches outline the respective pros and cons. To overcame limits of these methodologies a *Mixed-Holistic-Reductionist* approach are presented in [23]. With such approach one additional layer, called *Service*, is introduced in order to justify functional relationships between components and infrastructure at different levels of granularity. We can consider the *service* representation as well as a middle layer between the holistic and the reductionist capable to describe, for instance, services to customers and to other interconnected infrastructures. In this way both 'pros' approaches are maintained basically integrating three levels of abstraction into a single, flexible representation of the reality.

With the **MHR model**, relationships between infrastructures could be seen at different levels through either a top-down or bottom-up approach. A key element of operators is the quality of Services towards customers.

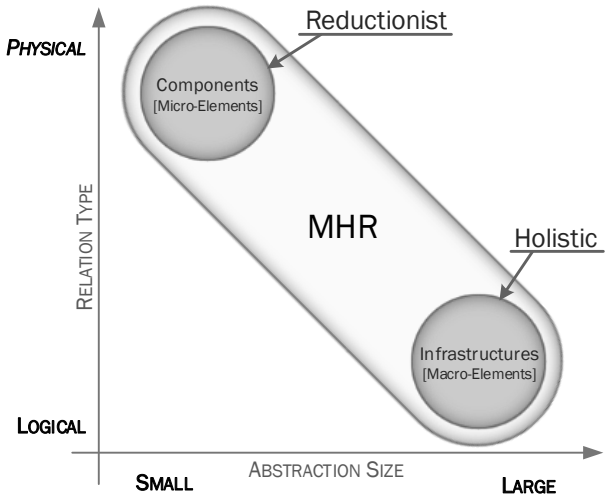


Figure 2.5 Graphical approaches comparison.

2.3 A Brief of Bayesian Networks

Starting to a probability distribution it is possible to build a *Bayesian Network* using rules of the probability for prediction, anomaly detection, diagnostic, decision making and so on, through time series and uncertainty conception. This capability is often used to express a probabilistic relationships among a set of variables taken into consideration. In a few words a Bayesian Network is a graphical representation which provides a full joint probability distribution model. Modelling thought statistical techniques have many advantages, like: represents dependencies among all variables, defines causal relationships giving the capability to better understand the problem domain enabling coexistence of both casual and probabilistic semantics. In a Risk Prediction (RP) a Bayesian Network (BN) provides a model in which include cascading probability between different entities in order to include a more accurate information about the actual reliability state of the analysed system. Using a BN we have the knowledge in a uncertain domain, which is a *directed acyclic graph*. This means that, all edges in the considered graph are *directed* and *cycles* that returns at a starting **are not**

allowed. This latter statement, as we will see, is very important to consider to correctly introduce portions of BN in a final RP model. Based on Bayes rules, such a graph express conditional relationships (arcs) among the different variable (nodes). In our specific case Nodes are represented by entities that could be modelling specific events due to defined vulnerabilities.

Through the **Bayes' Theorem** it is possible to describe the *probability* of a given *event* thanks to a priori knowledge. For instance, if a dangerous event it is associated to a possible sub-system fault, the information about the probability of sub-system fault could be used to better understand and asses the probability to have such a fault, compared with the probability to have the dangerous event without the possible faults knowledge. The Bayes rule is described by the following formula:

$$P(H \mid E) = \frac{P(E \mid H) \cdot P(H)}{P(E)} \tag{2.1}$$

where:

- $P(H \mid E)-$ conditional probability of H occurring given the *evidence* E;
- $P(E \mid H)-$ *evidence* E probability if the *hypothesis* H is true;
- $P(H)-$ priori probability of the *event*;
- $P(E)-$ priori probability that the *evidence* itself is true.

In general, given a set of nodes $X = \{X_1, X_2, ..., X_n\}$ a *Bayesian Network* is a network structure S which express a set of conditional independence assertions about variables in X and a set P of local probability distributions associated with each variable. Indeed, the **joint probability function** for any **Bayesian Network** is:

$$P(\mathbf{X}) = P(X_1, X_2, ..., X_n) = \prod_{i=1}^{n} P(X_i \mid X_1, X_2, ..., X_n) = \prod_{i=1}^{n} P(X_i \mid parents(X_i)) \tag{2.2}$$

where the *joint probability is the product of the probabilities* of the involved variable given its parents' values. We notice that we have only causal connections where each parent node causes an effect on its children.

2.4 A Brief of Fuzzy Logic

One of the main problems, of modelling complex systems, sometimes regards the impossibility to have deterministic information about the capability of a generic entity to produce specific quantities of outputs (resources, failures and/or capabilities) with respect to its internal states.

Represent partial information or uncertainties using Fuzzy mathematical framework is a feasible solution. Such an approach was already suggested in [**?**] where authors propose to express uncertainties associated to subjective information and data, allocating them, through use *Fuzzy Membership Functions* (MF). Although the concept provided by [**?**] is very useful, was not completely exploit its full 'modelling' potential. This because it is only focused on the event period, on the duration of a related outage and to represent dependency degree among different infrastructure. In MHR-RFB approach are proposed Fuzzy mechanisms in all those cases where probability information and what-if analysis evaluation are not sufficient.

From a logical-mathematical point of view a fuzzy class A is set of well-defined objects. An object belongs to the '*Universe of Discourse*' U. Commonly a set $A \subset U$ is characterized by the function:

$$\mu_A(x) = \begin{cases} 1 & \text{for } x \in A \\ 0 & \text{for } x \notin A \end{cases} \tag{2.3}$$

where $\mu_A(x) \in \{0, 1\}$, Hence $\mu_A(X)$ can assume only 0 or 1 as values. In Fuzzy mathematical framework $\mu_A(x)$ can take values in the interval $[0, 1]$. In this way is possible to move from a *Crisp MF* to a *Fuzzy MF* one. Introducing a Fuzzy set F as $F = \{(x, \mu_F(x))/x \in A, \mu_F(x) \in [0, 1]\}$ (membership function) through $\mu_F(x)$ is specified the degree to which any element A belongs to Fuzzy set F. Fuzzy inference process may divided into 5-steps:

1. Input variables **Fuzzification**;
2. Fuzzy operators application (**AND/OR**) on the **Antecedent**;
3. Application of the implication method from **Antecedent** to **Consequent**;
4. **Consequent** rules aggregation;
5. Output **Defuzzification**.

Most used inference methodologies are: *Mamdani* and *Sugeno*.

2.5 MHR-Rational Fuzzy Bayesian

A flexible methodology capable to represent complex scenarios it is advisable in a Critical Infrastructures context. It is mandatory to collect information and data from heterogeneous sources without loss reachable degrees of knowledge attempting a data normalization but, where possible, use it also to 'deduct' new valuable informations. This is the main concept that over the years of work in CI field have inspired the improvement of our models with a Risk Assessment point of view.

Starting from *MHR Approach*, are presented in detail, first the aforementioned layers (Holistic, Service, Reductionist) and then introduced other ones with the intent to provide a more complete methodology . Furthermore, due to the need and common

use of *probability* numbers, in the Risk Analysis context, a Bayesian Network model will integrated in the MHR approach.

In Figure 2.6 it is illustrated a generic representation of the improved MHR methodology. While *Performance Entity* and *Reaction Entity* are introduced as subcategories of the service level, the *Event Entity* represents a new one. Thanks to this last type of entity, as will be shown, it will be possible introduce the mathematical probability framework into the MHR model. In the next sections, all typologies of entities will be fully described.

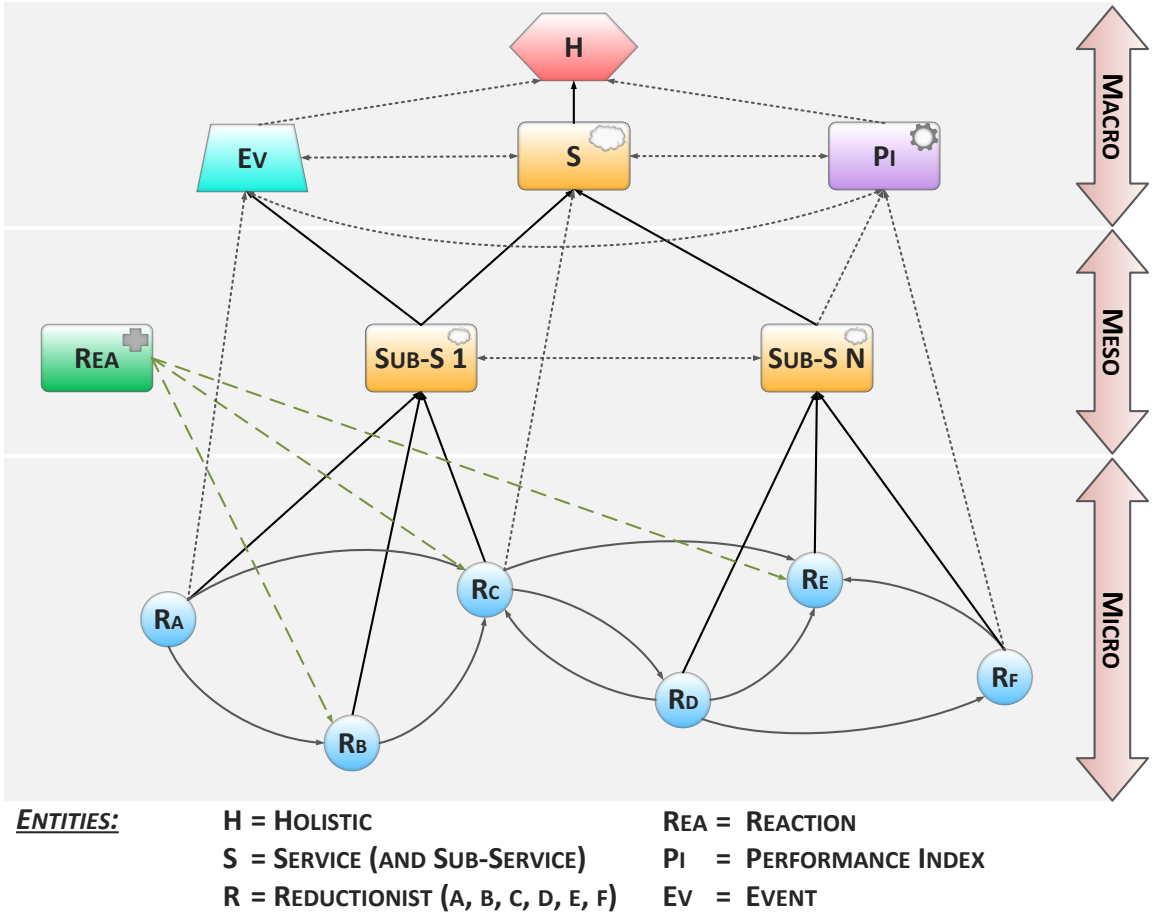


Figure 2.6 MHR-RFB representation.

Using Rinaldi's work in [22], we generically represent an entity like a graphical multi-level block. As in Figure 2.7 an entity is capable to receive in Input and then generate in Output *Resources*, *Failures* and *Capabilities*.

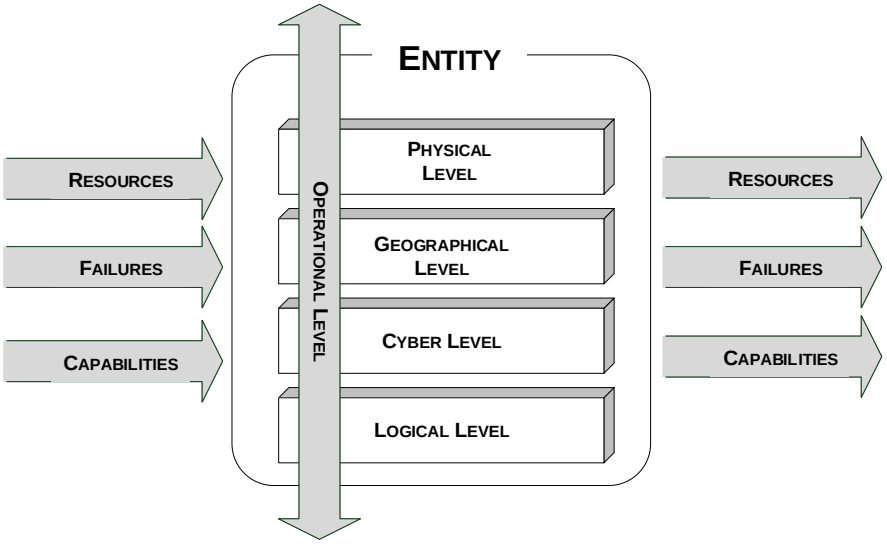


Figure 2.7 Generic entity representation.

We notice that in classic MHR approach only *Resources* and *Failures* are propagated. Because of the most recent projects, the need to represent a 'positive propagation effect' has encouraged the introduction of a new kind of entity Input/Output called *Capability*. An *Input* or *Output*, of an entity, can be modelled as:

- **Resource** – is any type of measure unit, variable, QoS (Quality of Service), Operational Level or information (simple or complex) with which any entity could represent its Input or Output as result of its own internal state and of all its possible external interactions with near entities.

- **Failure** – is a *negative* input or output, that is possible to quantify, with which every entity could produce (or receive) as result of unsuccessful procedures, damages, etc. or more generically, as a '*value*' able to produce loss effects.

– **Capability** – is a *positive* input or output, that is possible to quantify, with which every entity could produce (or receive) as result of successful procedures, mitigation strategies, etc. or more generically, as a '*value*' able to produce improvement effects.

As we know, each entity may '*exist*', at the same time, on different *dimensions/levels*. It is characterized by internal **State Variables** and each of these is usually correlated to dimension/level in which an entity interacts (see Figure 2.7). In short, a **State Variable**, represents instant by instant a specific state of the modelled entity with respect to the represented scenario. Finally, in function of its own Resources, Failures, Capabilities and its internal *States*, an entity, provides the most important state variable: the **Operational Level**. Thanks to its **Operational Level**, an entity, will be capable to produce predefined quantities of specific *Outputs*.

2.5.1 Reductionist Entity

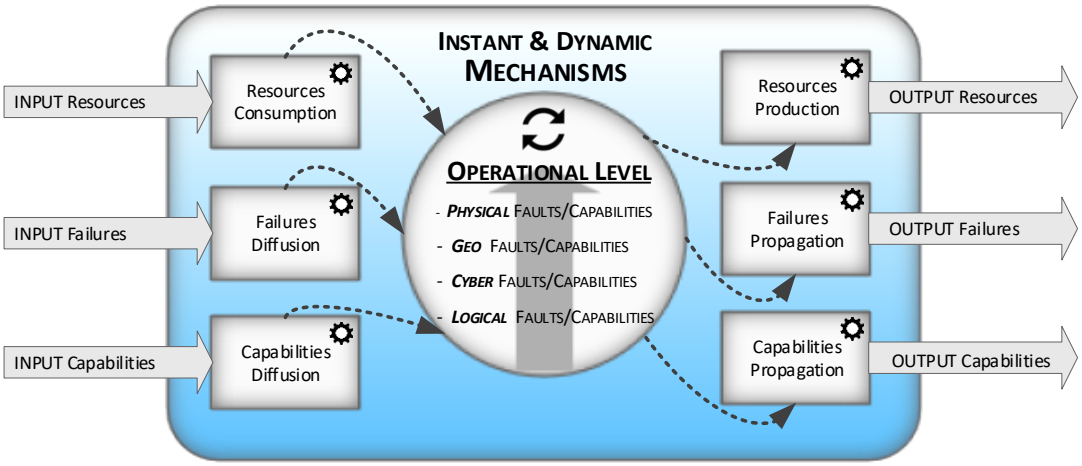


Figure 2.8 Reductionist entity representation.

A *Reductionist* block is an entity which "punctually" represents a specific element identified in a complex system. Considering a given granularity level (related to the

reference scenario information), it could be the whole component or the smallest significant fragmented part of it. For instance, taking into account an informational system, it is coherent consider a "Computer" entity without reach a useless high modelling detail level introducing its electronics components. From this perspective it is important to reach a certain "sensitivity" with respect to granularity that must be adopted in a modelling. We need to understand that the usability, completeness and clarity are aspects which make the complex world easier to understand. We can classify a *Reductionist* element as a *Micro-Level* entity (Figure 2.6).

As Illustrated in Figure 2.8 *Resources*, *Failures* and *Capabilities* are propagated towards the entity becoming its *Input*. They refer to the internal entity states and faults and its ability to produce resources or propagate failures and capabilities. These type of entities may receive Inputs and produce Outputs according to proximity with dependant reductionist elements of different nature too. Moreover, in specific case study, capability to have a high *Operational Level* depends also by the availability and quality of some aggregated resources and services provided by Reductionist and/or Service entities.

2.5.2 Service Entity

In Figure 2.9 a *Service* entity described as block is illustrated. Like the *Reductionist* block, the *Service* one is capable to receive in input *Resources*, *Failures* and *Capabilities*. Considering the intrinsic nature of a service it is possible to represent a system functionalities provided for a specific end-user. With such element we may provide: a higher level of failures and/or capabilities propagation, an intermediate representation between a Reductionist and Holistic layer and aggregate information, resources or variable of different nature that usually are not easy to represent. A *Service* element could be classified, with respect to the model needs, as a *Meso-level*

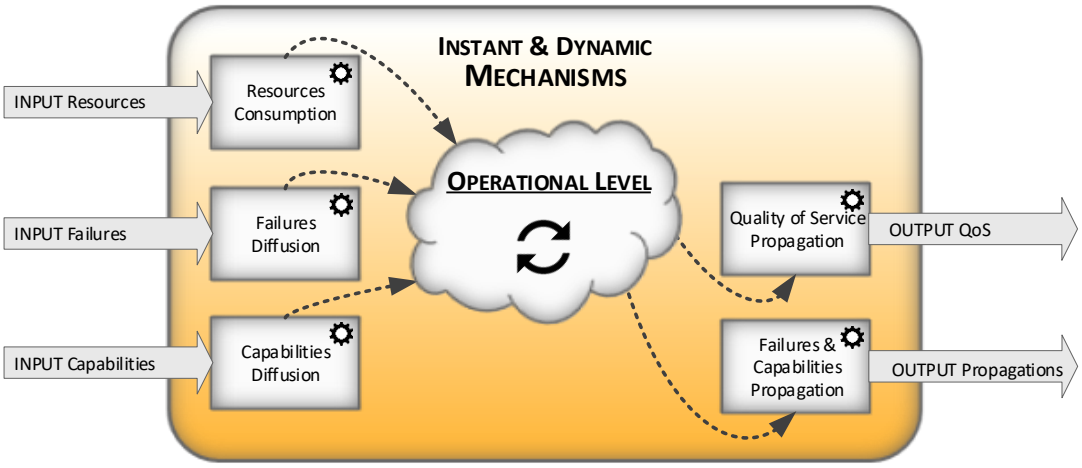


Figure 2.9 Service entity representation.

or *Macro-Level* entity (Figure 2.6). In some specific cases it is possible modelling a "hybrid" service/reductionist entities.

Performance Entity

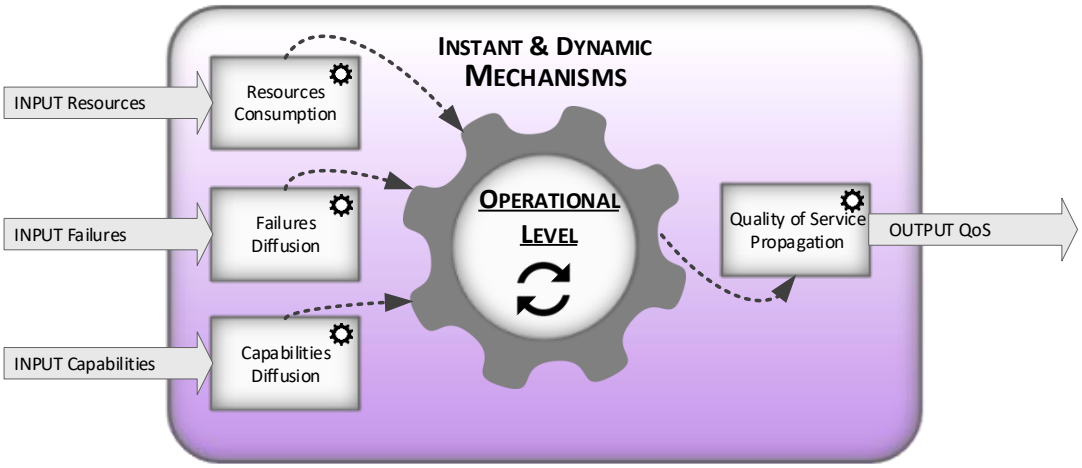


Figure 2.10 Performance Index entity representation.

The introduction of the service entity subcategory, called *Performance Index*, is proposed to improve the explanatory capabilities of the MHR model. In the economic

context, with performance index, is indicated a monitored progress that regards an organizational or business process. In this way, it will be possible recognize entities capable to calculate complex QoS metrics which express "performance" for specific aspect of a given infrastructure.

Reaction Entity

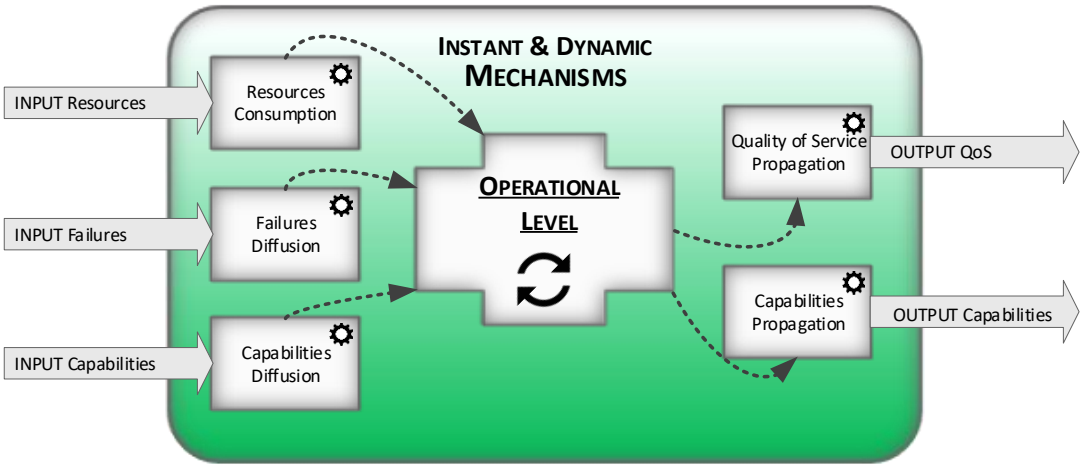


Figure 2.11 Reaction entity representation.

In some scenarios it is important to represent the '*diffusion*' of '*positive*' effects consequently to *reactions* or *mitigation strategies*. For instance, in natural disaster scenarios, represent "effort" which could be granted by local Civil Protection, provides a good level of information about preparedness degree in critical situations. For these reasons, a subcategory called *Reaction* entity was integrated in the improved MHR methodology. Such an entity can propagate, through its output, a QoS level (toward specific strategic elements of the considered scenario) or positive capabilities (with regards to its available resources and its operational level in a specific time).

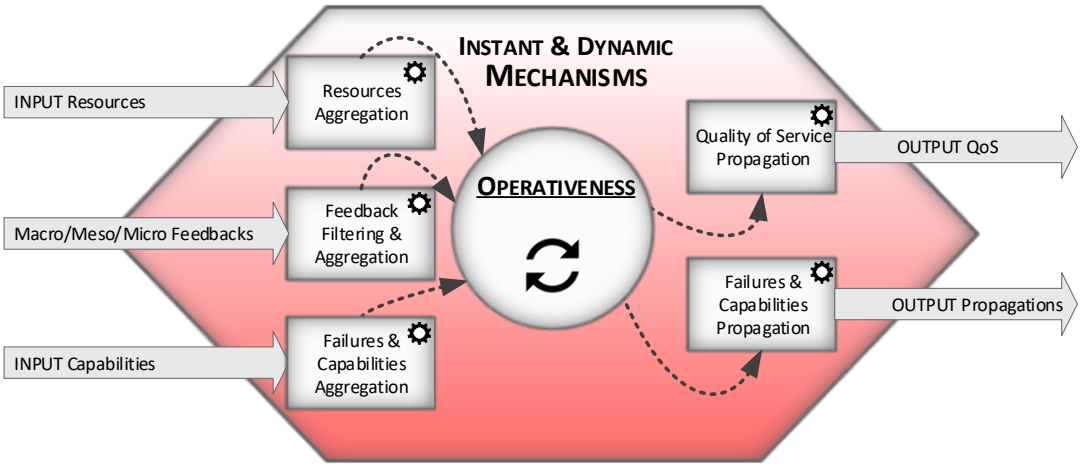


Figure 2.12 Holistic entity representation.

2.5.3 Holistic Entity

An *Holistic* entity is capable to represent global iterations among other complex systems. When we use the "Holistic" term, to better understand its meaning, we can consider the philosophical point of view. Holistic word root came from Greek language and it means '*Total*', '*Global*'. It was born in opposition to the reductionist philosophy, representing the inability of a complex system to express all the parts which compose it. Ideally, an holistic representation, *can not be expressed as the direct functional sum of all sub-systems which compose it.*

At this level, it is possible to model complex interaction mechanism also among macro, meso and micro elements and micro-components (of the same system), filtering and aggregating informations of different nature. In this case, through received failures and capabilities, we have the chance to modelling, for example, malicious behaviours or mitigation strategies effects, that might be very difficult to model with a different level of abstraction. Finally, a Holistic entity, calculating its operativeness, allows a high knowledge degree about the '*global*' status of the complex system itself. We can classify a *Holistic* element as a *Macro-Level* entity (Figure 2.6).

2.5.4 Event Entity

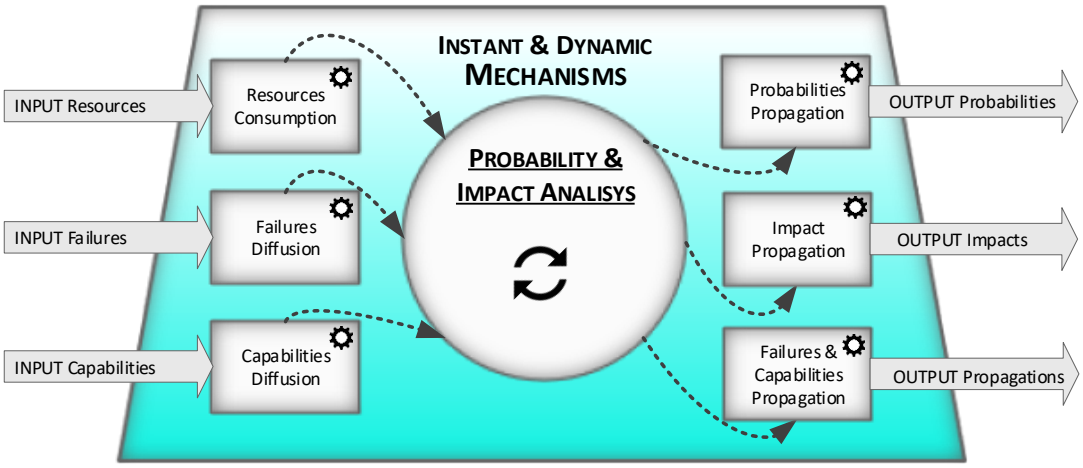


Figure 2.13 Event entity representation.

As shown in the next section, introduction of a new entity category, called *Event* entity, is mandatory in order to introduce the probability in the MHR Risk Analysis Framework. Concept of *Event* is totally different from the common MHR entities modelled as *Holistic*, *Reductionist* or *Service*. It is possible to define an *Event* entity when statistical historical data are available or when it is required evaluate impacts due to well-known occurrences. Whit this perspective, an *Event* entity, manages data concerning resources, failures and capabilities but also probability of a considered event and impact related to such an event.

Propagate failures, due to specific 'identified' events, provides a new tool for assessing risk and its consequences, in order to analyse possible solutions for reduce the exposure to it.

2.5.5 Introducing Bayesian Network in MHR-RFB Approach

As seen from the above, we can introduce the probability framework into an MHR model by using *Event* entities (Section 2.5.4) and concept provided by *Bayesian Networks*

(Section 2.3). Through a Bayesian Network example, we can better understand how is possible to apply this mathematical framework to a common CI model case study. We suppose to have a well-known risk about a possible dangerous event (H) which could be occurs in a involved critical infrastructure. Such event (H) might occur due to three possible fault in thee different subsystems (A, B, C) Figure 2.14.

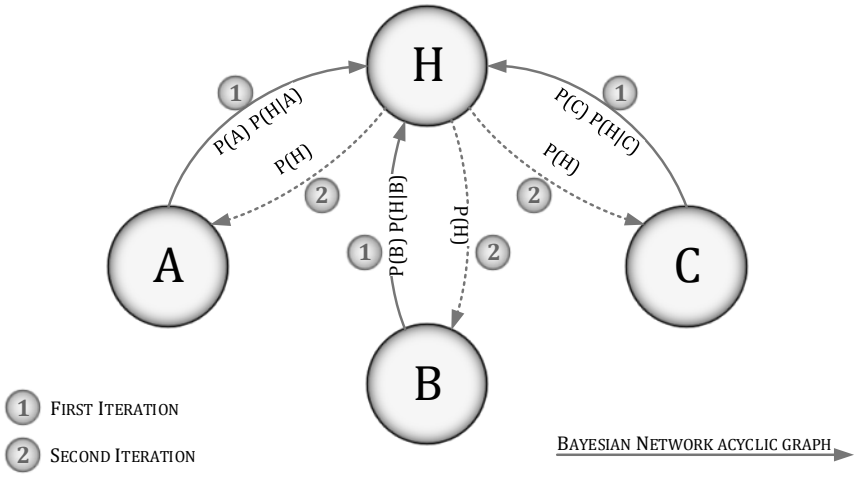


Figure 2.14 Bayesian-Network example.

In Figure 2.14 example we have functional dependencies among node H (Dangerous Event) and nodes A, B, C (Sub-systems Faults). The first iteration represents the real Bayesian-Network acyclic graph. Whit the second iteration $P(\mathbf{H})$ 'information' (calculated in the first iteration) it will redirect to A, B and C nodes. Thanks to formulas (2.1) and (2.2) and BN graphical representation we can reply to two different questions (using the two iteration):

1. Given priori probabilities of possible sub-systems faults $P(A)$, $P(B)$, $P(C)$ and their conditional probability of the event H - $P(H \mid A)$, $P(H \mid B)$, $P(H \mid C)$ (due to the occurrence of an evidence), what is the *joint probability* to have H - $P(H)$?

2. Given the calculated probability of event H - $P(H)$, what is the probability that it could be directly dependant on A, B or C - $P(A \mid H)$, $P(B \mid H)$, $P(C \mid H)$?

All starting knowledge can be summarized in following table:

Table 2.1 Bayesian Network probability knowledge.

	Conditioning H	**Fault**
A	$P(H \mid A)$	$P(A)$
B	$P(H \mid B)$	$P(B)$
C	$P(H \mid C)$	$P(C)$

We notice that the sum of conditioned probabilities ($P(A \mid H)$, $P(B \mid H)$ and $P(C \mid H)$) must be equal to 1 (100%). Then, using formula (2.2) we are able to reply to the first question calculating:

$$P(H) = P(A) \cdot P(H \mid A) + P(B) \cdot P(H \mid B) + P(C) \cdot P(H \mid C) \tag{2.4}$$

where each couple $P(E) \cdot P(H \mid E)$ is the probability to have H due to E. Introducing a subsequent iteration, where the $P(H)$ information is propagated towards fault nodes (A, B, C) and using formula (2.1) we are able to reply to the second question calculating:

$$P(A \mid H) = \frac{P(A) \cdot P(H \mid A)}{P(A) \cdot P(H \mid A) + P(B) \cdot P(H \mid B) + P(C) \cdot P(H \mid C)} \tag{2.5}$$

$$P(B \mid H) = \frac{P(B) \cdot P(H \mid B)}{P(A) \cdot P(H \mid A) + P(B) \cdot P(H \mid B) + P(C) \cdot P(H \mid C)} \tag{2.6}$$

$$P(C \mid H) = \frac{P(C) \cdot P(H \mid C)}{P(A) \cdot P(H \mid A) + P(B) \cdot P(H \mid B) + P(C) \cdot P(H \mid C)} \tag{2.7}$$

2.5.6 Introducing Fuzzy Logic in MHR-RFB Approach

Introduce Fuzzy concepts in MHR-RFB means, for instance, takes into account a generic entity and given its inputs, represent produced outputs due to internal states and fault levels. In Figure 2.15 is proposed a simple example of how it is possible to model a generic MHR-RFB entity behaviours using a Fuzzy Logic approach. It is considered an entity with 2 different inputs, capable to produce in output QoS (Quality of Service) and an internal Fault level.

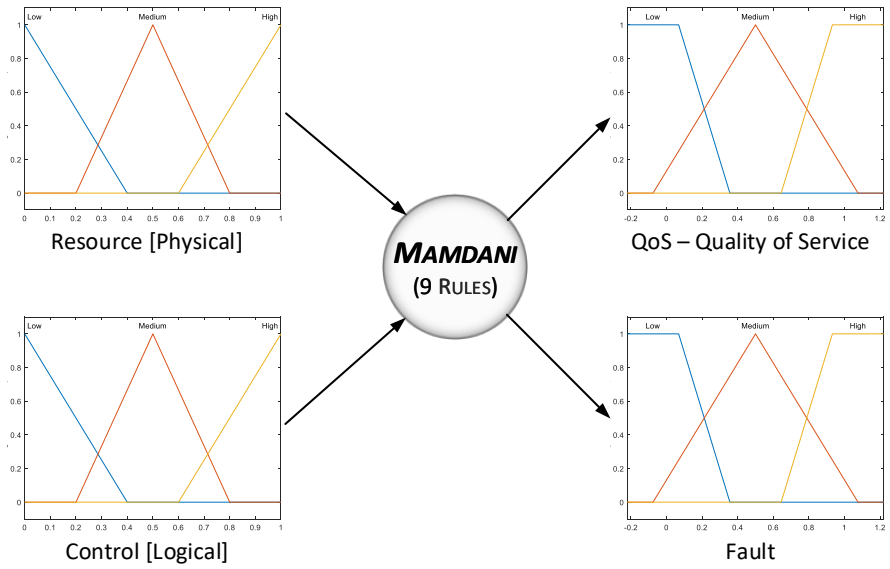


Figure 2.15 Modelling entity behaviours using fuzzy inference.

Thanks to the 'semantic nature', which characterize construction of a fuzzy logic, it is relatively simple to design *Fuzzy MF* (Figure 2.15) and **IF** [*Antecedent*] **THEN** [*Consequent*] rules. Such rules are strictly correlated to a domain expert interview.

In the example below, for 2 inputs, each one composed by 3 MF, we have to explicit 9-rules ($2^{(3)}$):

1) **IF** (R *is* **L**) **AND** (C *is* **L**) **THEN** (Q *is* **L**)(F *is* **H**)

2) **IF** (R *is* **L**) **AND** (C *is* **M**) **THEN** (Q *is* **L**)(F *is* **H**)

3) **IF** (R *is* **L**) **AND** (C *is* **H**) **THEN** (Q *is* **L**)(F *is* **M**)

4) **IF** (R *is* **M**) **AND** (C *is* **L**) **THEN** (Q *is* **M**)(F *is* **H**)

5) **IF** (R *is* **M**) **AND** (C *is* **M**) **THEN** (Q *is* **M**)(F *is* **M**)

6) **IF** (R *is* **M**) **AND** (C *is* **H**) **THEN** (Q *is* **M**)(F *is* **M**)

7) **IF** (R *is* **H**) **AND** (C *is* **L**) **THEN** (Q *is* **M**)(F *is* **H**)

8) **IF** (R *is* **H**) **AND** (C *is* **M**) **THEN** (Q *is* **M**)(F *is* **M**)

9) **IF** (R *is* **H**) **AND** (C *is* **H**) **THEN** (Q *is* **M**)(F *is* **M**)

According with **IF** [*Antecedent*] **THEN** [*Consequent*] *Rules*, an expert system is able to get inputs information, compare and finding a match with the Antecedents expressed in provided rules as in Figure 2.15.

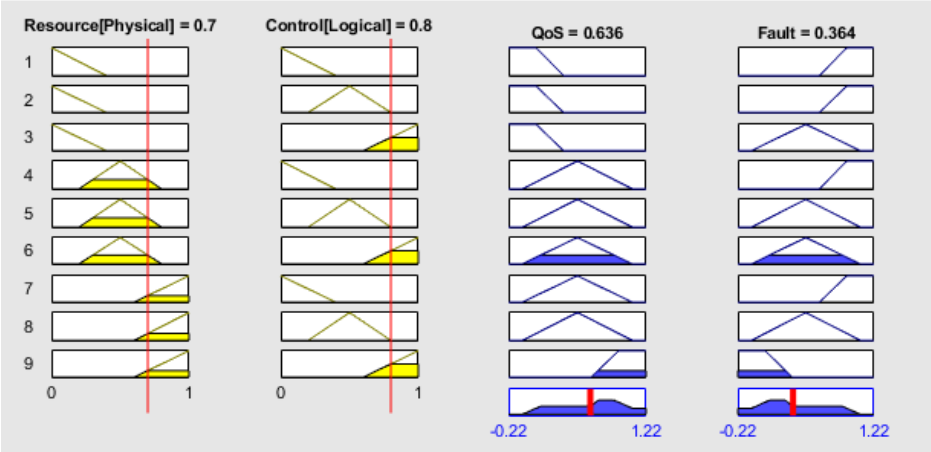


Figure 2.16 Fuzzy inference output.

Rules, which express expert knowledge basis, represent synthesis of what has been learned studying: a specific case study, taking into consideration similar systems data or through a 'verbal' description by a human expert.

2.6 MHR-RFB methodology application.

In this section it is presented an example of how MHR-RFB methodology works and how it is possible to use different mathematical framework at the same time in a unique modeling technique. We mainly represent an entity like a block divided into three sub computational parts: Input, State and Output. Each one of them is delegated to calculate and manage, in different manners: resources, failures, internal states, operativeness and capabilities to produce something in output (see Figure 2.17).

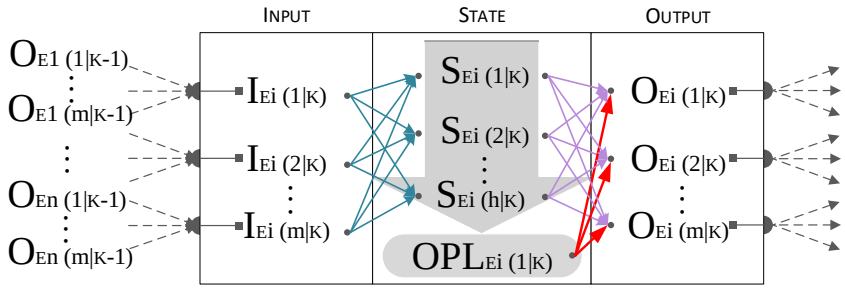


Figure 2.17 Input-State-Output entity mechanisms representation.

Given a complex system model composed by $\#n$ entities, $\#m$ typologies of input/output and $\#h$ internal states we generally express the i^{th} *entity*, dependent by $\#m$ *entities* (due to some propagated resources, failures or capabilities) in input, at the k^{th} *step* ≥ 0, with the formulas that follow in order to express Inputs (I), Internal States (S_T), Operational Level (O_{PL}) and Outputs (O):

$$I_{(Ei)}(w|k) = f(\ O_{(Ej)}(1|k-1), \ldots, O_{(Ej)}(m|k-1)\ ) \tag{2.8}$$

for $j \neq i$, $i = 1, \ldots, n$, $j = 1, \ldots, n$ and $w = 1, \ldots, m$.

$$\begin{aligned} S_{T(Ei)}(l|k) = f(\ & S_{T(Ei)}(1|k-1), \ldots, S_{T(Ei)}(h|k-1), \ldots, \\ & I_{(Ei)}(1|k), \ldots, I_{(Ei)}(m|k)\ ) \end{aligned} \tag{2.9}$$

for $l = 1, \ldots, h$

$$O_{PL(Ei)}(k) = f(\ S_{T(Ei)}(1|k), \ldots, S_{T(Ei)}(h|k)\ ) \tag{2.10}$$

$$O_{(Ei)}(w|k) = f(\ O_{PL(Ei)}(k), S_{T(Ei)}(1|k), \ldots, S_{T(Ei)}(h|k)\ ) \tag{2.11}$$

for $w = 1, \ldots, m$

To initialize the iterative calculation process for each i^{th} *entity*, starting with $k = 0$, we need to define all initial internal states as:

$$S_{T(Ei)}(l|k-1) \text{ for } i = 1, \ldots, n,\ l = 1, \ldots, h$$

and all Output:

$$O_{(Ei)}(w|k-1) = 0 \text{ for } i = 1, \ldots, n,\ w = 1, \ldots, m.$$

In (Figure 2.18) it is provided a simplified case study which take into account a portion of a generic organization model. We can image to start representing organization as a holistic point of view. This holistic perspective will give us a global 'health' state metric about the organization 'system'. In order to enrich this global evaluation we need to correlate it to QoS produced by its department (in figure Assets 1,3,6) and the probability which a critical event occurs.

2.7 MHR-RFB Risk Analysis Interpretation

Through a Risk Analysis terminologies process (see Chapter 1), it is interpreted the MHR-RFB approach. Using this modelling technique a **IDRA** (*Informed Dynamic Risk Analysis*) methodology is proposed to understand how it is possible to extend a classic '*static*' Risk Analysis approach to a more modern '*dynamic*' interpretation of Risk in which it could change its state and nature during its evolution in time.

The proposed Risk Analysis framework starts identifying all involved strategical '*Assets*' in a well-defined scenario (Figure 2.18). Once these '*sensible*' aspects, of a given complex system, are outlined, a '*Hazards*' Analysis, with respect to all mentioned layers (Physical, Geographical, Cyber, Logical and so on), helps to classify *sources of possible dangers*, in other terms: '*the prerequisite of the Risk*'. Subsequently, it is possible to move toward a more deeper process which consists to punctually assess '*Threats*'. With '*Threat*' we express what which '*triggers*' a specific '*vulnerability*' through the action, whether or not consciously, of a '*Threat Actor*'.

To better understand these first steps, we can imagine a scenario in which an IT asset suffer from important cyber vulnerabilities. In this context a '*Cybercriminal*' (Threat Actor) is able, through a Cyber Attack, to exploit a specific system '*Vulnerability*'.

Following the MHR model, triggering the '*Threat*', the asset '*Impact*' is evaluated first and then, due to a '*vertical*' propagation effect (see Figure 2.18 path form the

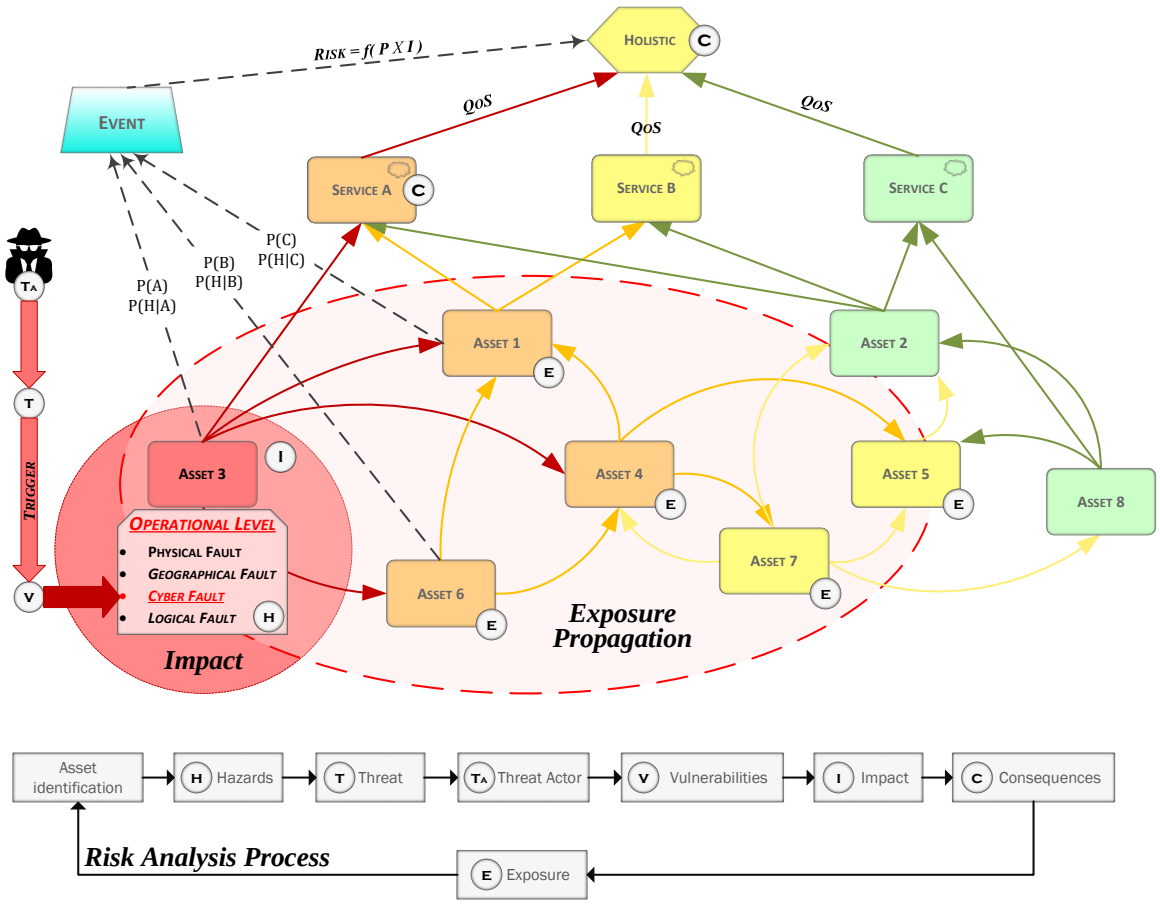


Figure 2.18 MHR Risk Interpretation.

reductionist entity to service and finally to holistic system point of view) all consequences are estimated. Moreover, thanks to (inter)dependencies and associated '*Cascading Effects*', it is possible to understand the consequent '*Risk Exposure*' which is directly correlated to the risk source proximity. Back at the start of the Risk Analysis (to the Asset Analysis), this iterative process can be followed as long as necessary in order to complete the whole scenario risk evolution.

At this point, it is very simple to understand how the proposed methodology provides an approach which fits the needs of modern real-time systems dealing with the perceived risk in a real-time context. Making a final simple distinction, we can say that with a classical Risk Analysis approach it is possible to introduce in an information system an off-line tool while adopting approach proposed in this work, it is possible to introduce a new generation of on-line tools able to supply a continuous decision support system to operators and to all other end-users typologies.

Chapter 3

CISIApro simulative approach

This section describes the main features of the CISIApro simulator, including its reliance on the mixed holistic reductionist (MHR) approach proposed in Section 2.5. Furthermore, such chapter deals with Risk Assessment methodology introduced in a defined software and hardware environment. CISIApro simulator (Critical Infrastructure Simulation by Interdependent Agents) has been designed for analysing the short-term effects of failure both in terms of faults propagation and with respect to performance degradation. Following, a brief summarization of the CISIA software evolution over the years:

- First implementation of a **CISIA** framework was found in [25](2004) thanks to Panzieri, Setola and Ulivi works. Authors describe this tool as a simulator able to analyse short term failures effects due to resources propagation and performance degradation. This first version was based on Recursive Porus Agent Simulation Toolkit (Repast) open-source agent-based development software.

- Then in [26](2008) a new modelling framework was presented. In this **framework**, **CISIA** is a C/C++ software classes, which once programmed and compiled, creates a package files and an executable file.

- In its last releases **CISIApro** (first version in 2014) is a tools platform completely redesigned by C.Palazzo [27] in order to have best simulation time performances (from the order of minutes with CISIA firmware into milliseconds/seconds with CISIApro) and to improve complexity of modelled scenarios.

Typically, Risk Management deals with the use of mathematical techniques not always able to handle the dynamic associated with the risk evolution. The main objective of the proposed framework, is to provide a flexible methodology able to exceed the limits of other existing approaches, achieving a proper level of complexity. From this perspective, CISIApro represents a good solution to assess risk due to resources/failures/capabilities propagation also considering cascading effects.

3.1 Critical Infrastructure Simulative Approaches

Satumitra and Dueñas-Osorio [28] have published an exhaustive survey of the principal methods for critical infrastructure modelling and simulation. Their survey reveals that most of the approaches for dealing with infrastructure interdependencies, cascading system failures and risk mitigation are complementary rather than competing. The modelling approaches include techniques based on game theory, graph theory, risk-based models, Petri nets and Bayesian networks. However, many of the interdependency models are primarily conceptual in nature or are limited to simple or high-level scenarios.

Rahman et al. [29] have developed the Infrastructure Interdependency Simulator (I2Sim) based on the well-known cell-channel model. In this model, infrastructures and their interconnections are represented using cells and channels. A cell is an entity that performs a function. For example, a hospital is a cell that uses input tokens such as electricity, water and medicines, and produces output tokens such as the number of patients served. A channel is a means through which tokens flow from one cell to another. The interdependencies between infrastructures are non-linear relationships

that are summarized in the form of human-readable tables. I2Sim helps decision makers optimize resources and prioritize system restoration actions after critical events. I2Sim is the core element of DR-NEP (Disaster Response Network Enabled Platform), an advanced disaster management tool that is based on a web services infrastructure and incorporates domain simulators. The modeling technique has been validated by several case studies, including one involving the Vancouver 2010 Winter Olympics. However, the case studies mainly focus on natural disasters and do not consider the impacts of cyber attacks.

A survey of the research literature reveals that the majority of simulators employ the agent-based paradigm, in which a population of autonomous interacting agents coordinate their decisions to reach a higher-level global objective. Each infrastructure is modeled as an agent. Interdependencies are modeled as edges between agents. This enables agents to exchange information: each agent receives inputs from other agents and sends its outputs to other agents (see Nieuwenhuijs et al. [30] for further details). The CISIApro (Critical Infrastructure Simulation by Interdependent Agents) simulator used in this research employs the agent-based paradigm, where each agent has a high-level description of the internal dynamics of an infrastructure. The main goal of CISIApro is to study the propagation of faults/attacks and the resulting degradation in performance.

Another recent trend is the use of co-simulation frameworks, where several domain-specific simulators are connected using a well-defined and generic interface (API) for simulation interoperability [31]. The main goal of a co-simulation framework is to reuse existing models in a common context to simulate complex scenarios. The Mosaik ecosystem [31] has been applied to analyse a smart grid scenario in which telecommunications network and power grid simulators are integrated. This work integrated various simulators for the electrical side, including models of electric vehicles

in Python, photovoltaic cells in MATLAB/Simulink, residential loads as CSV time series data and two power distribution grids in Python. Mosaik is still at an early stage of development, but it can cope with different temporal resolutions (e.g., continuous, every minute or every fifteen minutes).

3.2 CISIApro Description

CISIApro is an agent-based simulator, where each agent has the same structure, see (Section 2.5). An agent receives resources and failures from other agents. A resource is a good, service or data produced and/or consumed by an agent that is represented in CISIApro as an entity. The ability to produce resources is summarized by the concept of an operational level, which depends on the availability of received resources, propagation of faults or capabilities and functionality of the entity itself. An entity also receives failures via its upstream interconnections and spreads the failures to downstream entities. The failures propagate different types of faults in different ways. The output of an agent depends on the actual value of the operative level. The considered "interdependencies" calsses are: physical, logical, geographical and cyber.

CISIApro simulator was developed to overcome certain implementation problems associated with the old CISIA framework. The main problem was the possibility of an infinite loop when resources are instantly exchanged between entities. CISIA's main cycle buffers all the information exchanged between entities at each time step. If the exchanges form a cycle, then the simulation time step never ends, which results in an infinite loop.

In CISIApro simulator, the information flow is well defined with a threshold of maximum executions in a time step to avoid endless loops. Moreover, for each entity, the following variables are evaluated:

1. the received resources and faults/threats from upstream entities;

2. the dynamic evolution, if needed, where the evolution is depending on the time variable;

3. the instantaneous evolution behaviour, which happens immediately without the time dependency;

4. the resources and the faults/threats sent to downstream entities.

The difference between instant and dynamic evolution is due to the nature of fault to be propagated. For instance, the contamination of chemical product on a water pipe has a dynamic nature due to diffusion time; the consequences of a cyber-attack can also depend on the persistence of the attack and then on time; electricity in a power grid could be modelled as an instant propagation through the power distribution system wires.

In CISIApro, a graphical user interface (Figure 3.1) is provided to create and connect entities and to add the exchanged resources in an efficient manner.

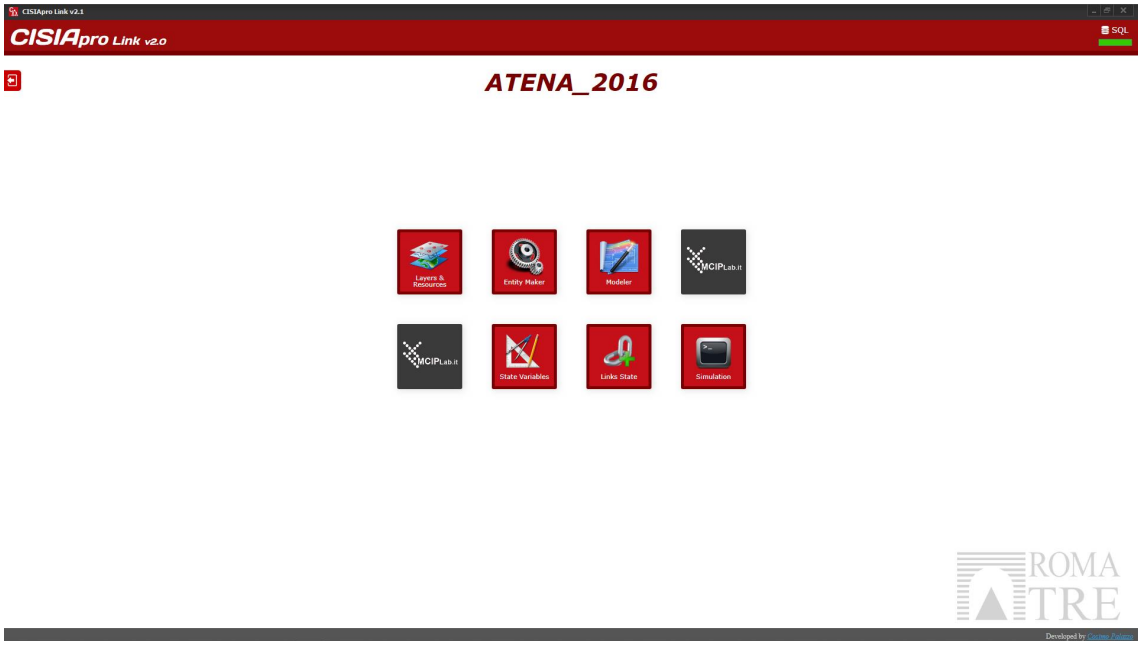


Figure 3.1 CISIApro user interface.

3.3 CISIApro Architecture

To redesign and implement the new CISIApro software it was necessary deal with specific "strategical" choices about the software technologies needed. This kind of choices were taken in order to have an added-value software, usable and scalable with respect to possible Critical Infrastructures scenarios to model. CISIApro is designed using particular programming techniques which allow use of common programming languages like C/C++ and languages that are used to create web/cloud platform . Although it might seem “a controversial choice”, it support a high productivity, usability and scalability along with the capability to integrate third parties software in the same architecture.

For the implementation of the CISIApro simulation engine, it was adopted a combination of PHP language (server-side programming language) with C++ compiling techniques. This is possible because PHP libraries was created through a C/C++ implementation. While, for the graphical interfaces it was used client-side JavaScript programming techniques. The main difference between C/C++ and PHP lies in the fact that C/C++ is a compiled language while PHP is an interpreted language. Thanks to PHP interpreter, inside CISIApro, is possible to implements all the behaviours and mechanisms of a modelled entity.

Below, are summarized some typical advantages by implementing entity using PHP programming language:

- to instantiate a variable in PHP it is sufficient to assign a value;
- the declaration of the variable type is implied when assigning a value;
- a variable can also be removed in the course of the script (through education unset ($ variable));
- the a variable "type" can be changed during the script execution;

- it is possible to use the object-oriented programming;
- PHP implements more than 90% of C/C++ functions without mentioning the countless available classes developed by its community.

As just previously mentioned, one of the possible approaches, which can be implemented in CISIApro, is the MHR modelling (Mixed Holistic-Reductionistic). This approach allows us to put information into a right level of detail with minimal data collection techniques obtaining meaningful knowledge. Starting with this perspective some guidelines were defined in order to design an improved simulation software:

- Each infrastructure is modelled from its macro-components, is to say, objects with a specific role, easily recognizable and whose overall behaviour is given by their interactions;
- A correct level of abstraction enables a consistent description of the modelled entities even if such information are based on generic and incomplete data due to the sharing information problem;
- Entities must be described in order to be confined and decoupled from each other. This because their behaviours should dependent only by values "explicitly" exchanged with other near entities.
- The simulation software must not impose any kind of limitation to representable behaviours in order to have the most appropriate representation of the reality. In addition, the size/scale of a given system should be free and at the same time bound to the needs of a specific case study.

With the use of the MHR layers is possible to capture the interdependencies among the different infrastructures. Each layer of the infrastructure is composed by several elements (blocks). All the elements showing characteristics within these layer follow a common general pattern:

– some elements have the capability to provide and / or consume resources (goods, services, etc.);

– some elements may be subject to failure or malfunction;

– different resources, faults and capabilities can be propagated in according to other elements 'proximity' (sometime of different nature);

– the capability of each element to provide the necessary resources directly depends on its own "Operational Level". In its turn, the Operational Level is related to resources availability received failures and capabilities.

It is important to understand that the idea behind modelling a critical infrastructure using CISIApro is both simple and effective. It consist in to define a complex simulation model, without having to define the input and/or output of specific entities, but simply defining the initial presence of faults and the initial state of the operational levels of the considered entities. In Figure 3.2 is illustrated the flow diagram of CISIApro which represents the logical schema at the basis of the CISIApro simulation engine.

CISIApro uses a database to capture all the information needed to represent multiple critical infrastructures and their interconnections. In addition, it is designed over different database structures to discern the construction design phase to the output storage. In this way, the information provided by CISIApro can be easily shared with other additional modules. Figure 3.3 shows the database structure. The DB stores the information needed for the representation of several Critical Infrastructures, such as:

- Each entity is a specific instance of an entity type;
- Each entity has a status made of variables with values;
- Each entity has ports for exchanging resources;
- Each resource is associated with a MHR layer/net;

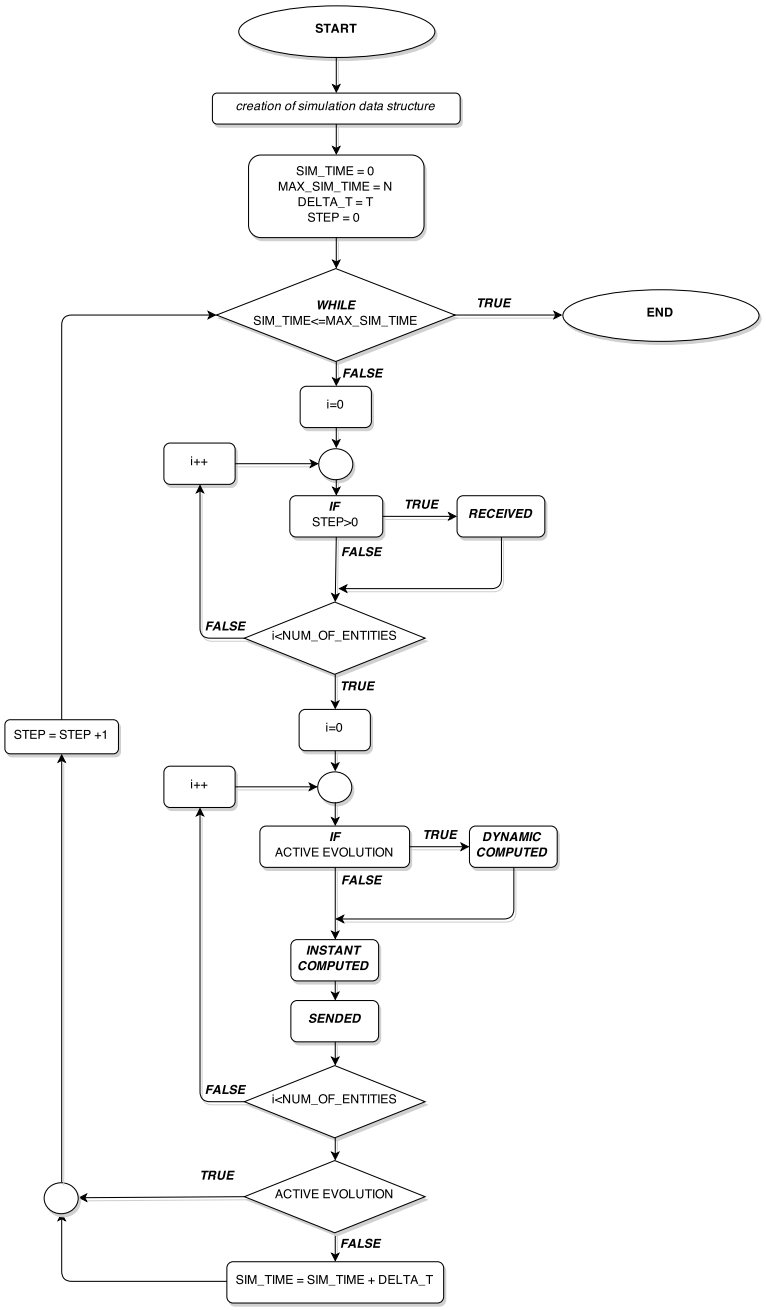


Figure 3.2 CISIApro simulation engine flow diagram.

- Each layer has proper interdependencies;
- Each interconnection is made of a couple of ports, associated to two entities.

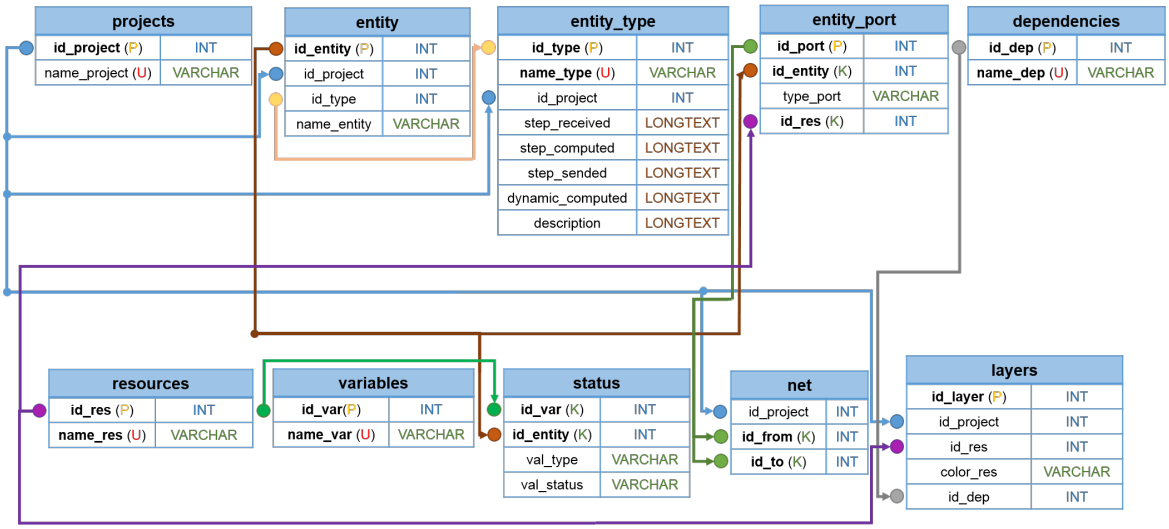


Figure 3.3 CISIApro database representation.

Outputs of CISIApro are stored in a different database with specific features, see Figure 3.4, such as the record time-stamp in terms of date, time and milliseconds. In this way, any downstream module can retrieve data regarding the latest actualized critical situation in the modelled scenario. Adjacency matrices which represent interdependencies existing between entities are generated during the design phase. During the simulation, the matrices are represented as queue data structures to speed up computations.

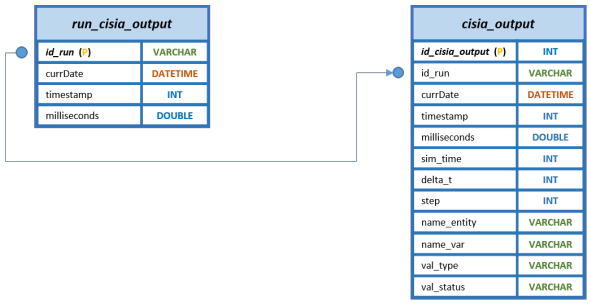


Figure 3.4 CISIApro simulation output database representation.

3.4 CISIApro Software Modules

We mainly split CISIApro into two software components: the first one is the software with which it is possible to design the CI model, given a certain scenario, and the second one, called CISIArun, represents the real simulation engine. Such engine can be integrated in a more complex software architecture. In this section it is presented a brief description of the main modules provided by CISIApro to exploit the potential of proposed modelling techniques and tools.

3.4.1 Layers & Resources Module

Thanks to the *Layers & Resources* module (Figure 3.5) it is possible to instantiate all the required layers in a critical infrastructures scenario model. It is the first step for the simulation implementation. Assign a specific resource to a corresponding dimension also gives us a deeper awareness with respect to the nature of the managed information.

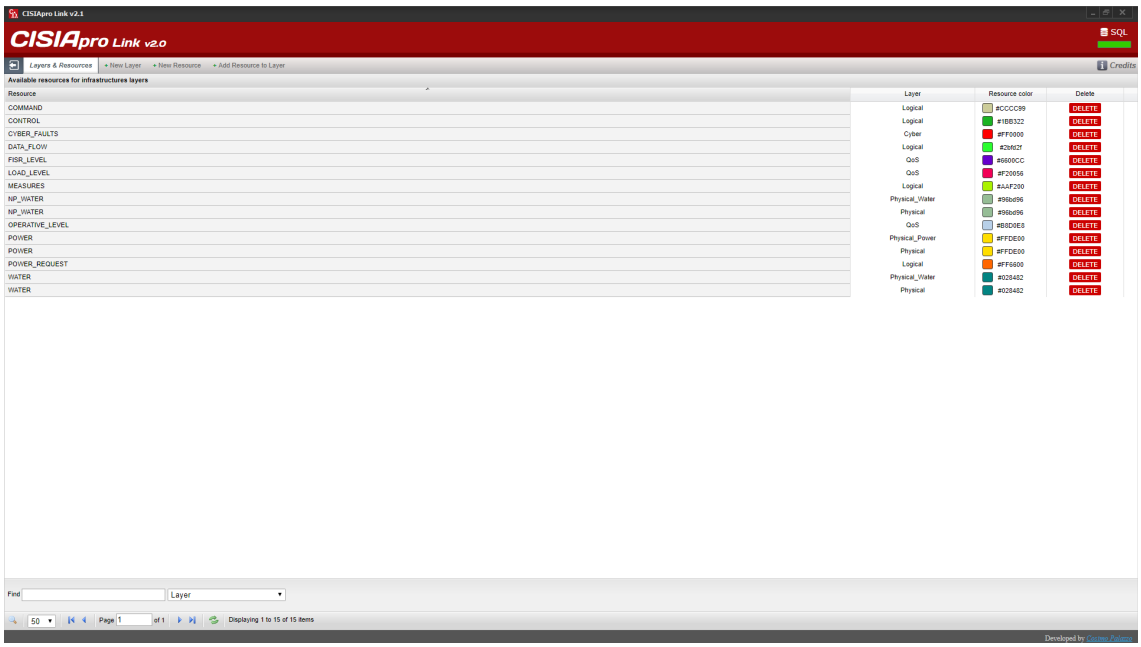


Figure 3.5 CISIApro module: Layers & Resources.

3.4.2 Entity Maker Module

In the *Entity Maker* module (Figure 3.6), using the integrated PHP code editor, it is possible to instantiate and programming behaviours for each considered entity class. Once completed this step, the introduction and duplication in the design phase (Section 3.4.3) will be allowed.

Each entity class is composed of four modules that are executed, several times, during the simulation run:

(i) RECEIVED, which evaluates the received resources and faults;

(ii) DYNAMIC COMPUTED, which implements dynamic evolution;

(iii) INSTANT COMPUTED, which implements instantaneous evolution;

(iv) SENT, which evaluates the resources that are sent to the downstream entities.

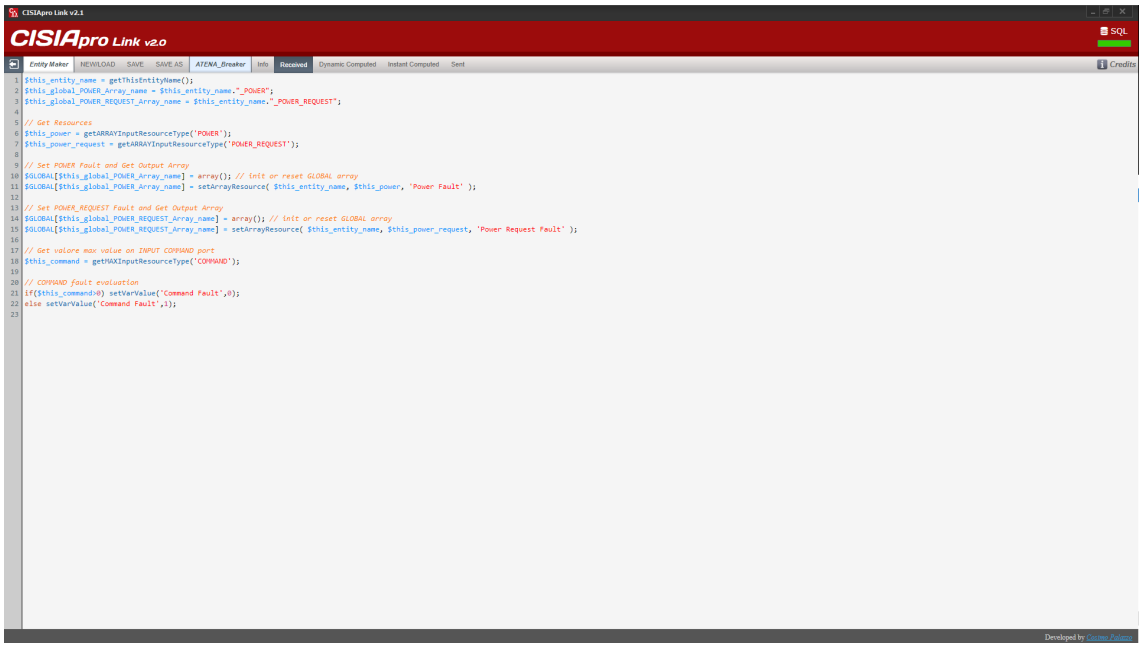


Figure 3.6 CISIApro module: Entity Maker.

3.4.3 Modeler Module

The *Modeler* module (Figure 3.7) is designed in order to improve the productivity in modelling Critical Infrastructures scenarios. Thanks to a usable graphic interface and a Drag & Drop system, it is an easier operation to introduce entities and create (inter)dependencies.

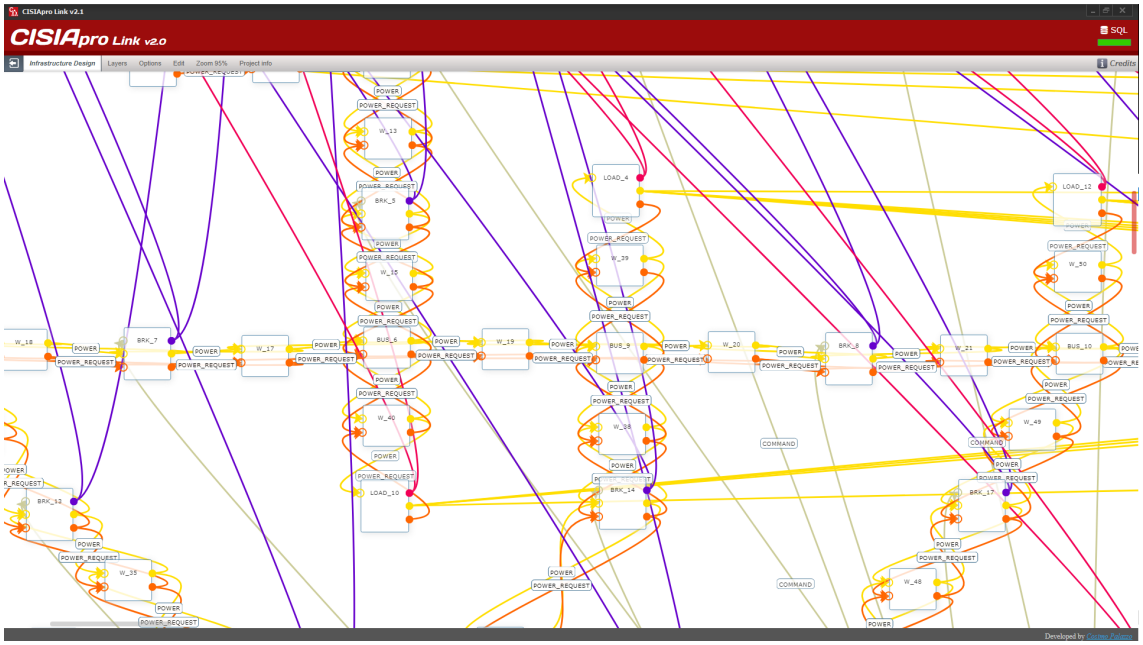


Figure 3.7 CISIApro module: Modeler.

3.4.4 State Variables Module

As previously mentioned, with CISIApro simulation, defining Input and Output is not required. This is possible because they are calculated, instant by instant, during the simulation time, with respect to entity *state variables* and especially evaluating *operational levels* related to each modelled element. In *State Variables* module (Figure 3.8) indeed it is possible to set the initial state for every variable that is part of the simulation.

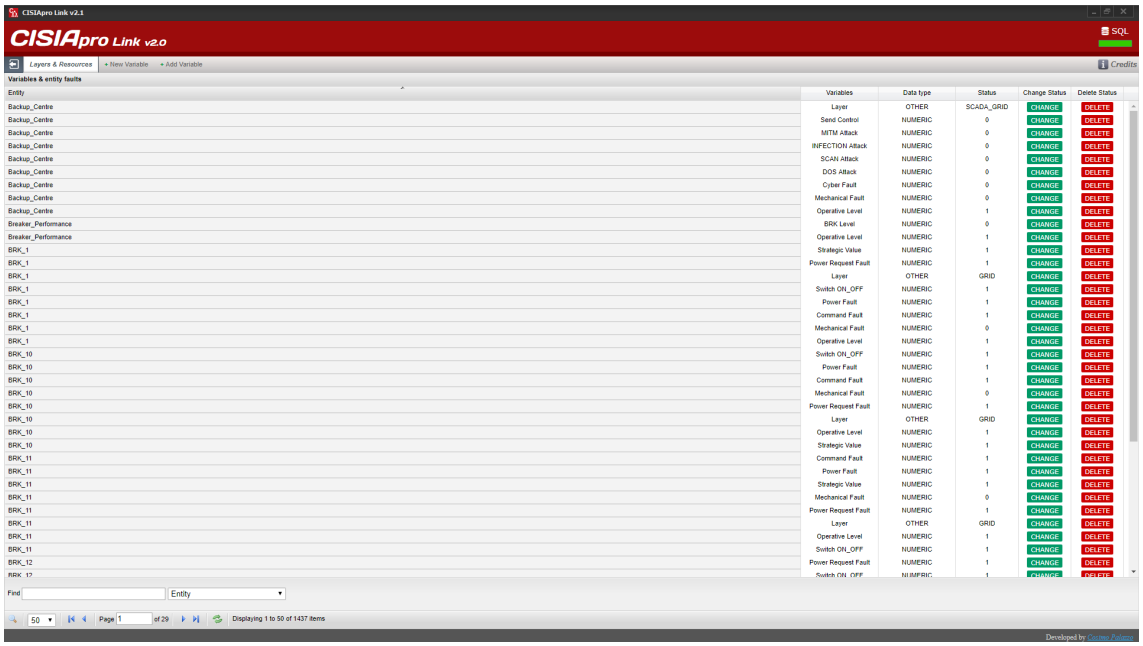


Figure 3.8 CISIApro module: State Variables.

3.4.5 Link States Module

Link States is the most recent module tool introduced in CISIApro software (Figure 3.9). Such module was designed in order to be compliant to model in which dynamic links are required. A dynamic link is defined as a link that connects two entities to each other, that could change its state during different simulation. For instance, it allows to model scenarios, like transportation infrastructures, where an entity may represent a transport (airplane, bus, train and so on) and links represent multiple available paths. Through this mechanism it will be possible to instantiate all the multiple connection, among the involved entities, activating only one of them at a time.

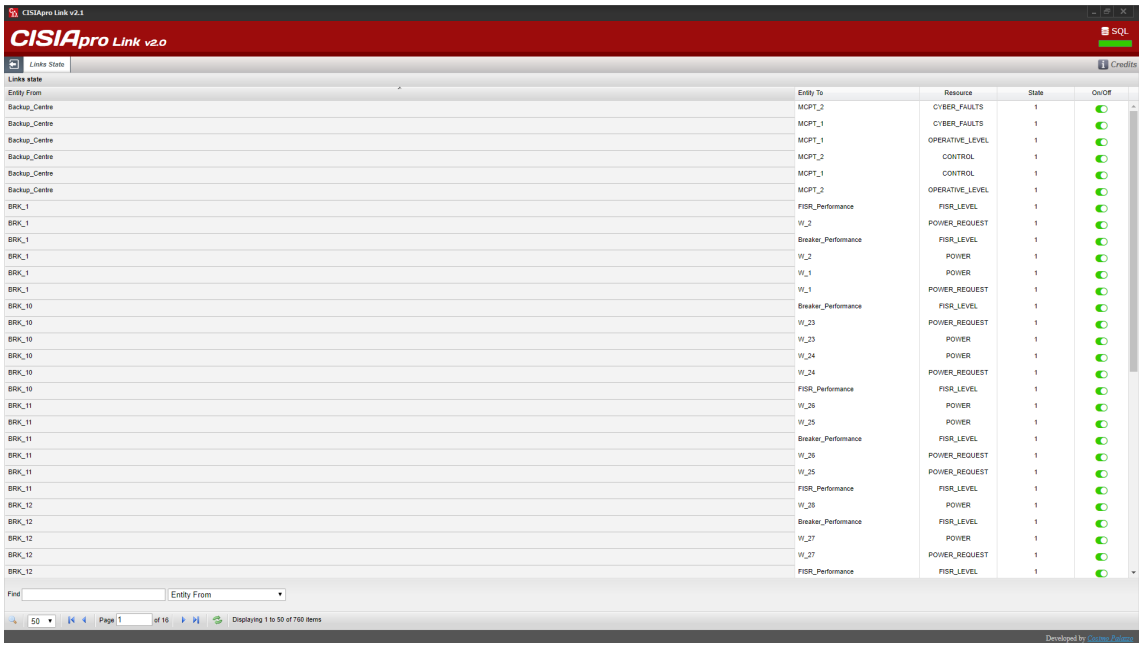


Figure 3.9 CISIApro module: Link States.

3.4.6 Simulation Module

Thanks to the *Simulation* module (Figure 3.10) is possible to debug a simulated scenario, validating its results and performances before proceeding to the production phase.

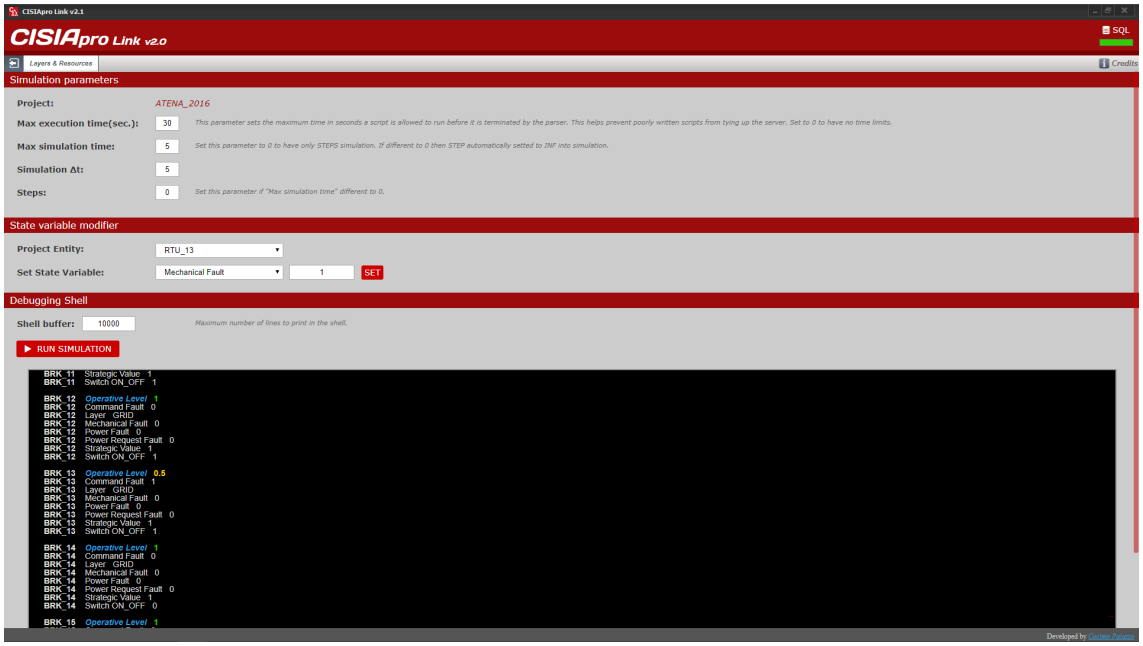


Figure 3.10 CISIApro module: Simulation.

3.5 CISIApro engine and introduction of a new '*Spatial Propagation*'

CISIApro engine represent the real software strength along with the ease offered in modelling complex systems. The engine consists in an agent-base simulation based on evolutionary algorithm model where each '*agent*' is able to receive and propagate resources, faults and capabilities (see Section 2.5). Under this perspective it is possible to trace back to a multidimensional graph wherein each '*dimension*' represents a graph in which a '*resource*' can be propagated among involved entities (Figure 3.11).

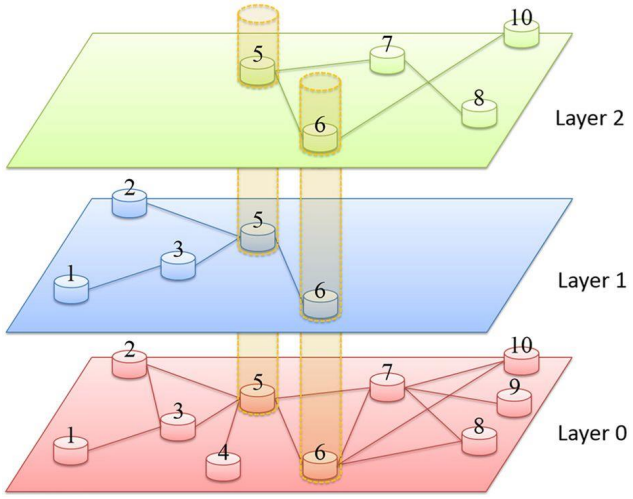


Figure 3.11 Propagation model on a multidimensional graph representation.

As represented in Figure 3.11 some entities can exist at the same time, with its own evolution, on different dimensions. This means that through such resources propagation, on different layers, entities could affect each other.

Two different '*steps*' can be mainly identified in the engine simulation. The first one regards a micro-step (*instant evolution*), the second one, instead, is represented by a macro-step (*dynamic evolution*). Hypothesizing a time-line evolution for each entity (see Figure 3.12), until an active evolution persists the micro-steps are incremented

and the instant behaviours computed. Once all inputs/outputs converge to a stable solution the macro-step (dynamic computation) can be calculated and incremented of a Δt.

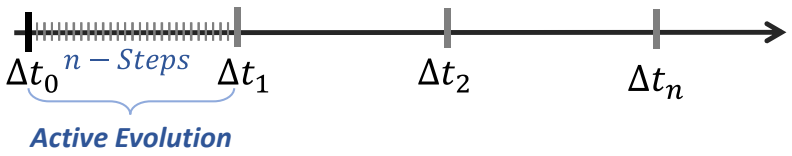


Figure 3.12 Entity time-line steps evolution.

For this kind of simulation it is not possible to know, a priori, the precise number of needed steps to converge to the final solution. Therefore, it is very important to be careful not including dangerous '*Logical Loop*' which could bring to a simulation divergence.

During this work a lot of improvements were conducted in order to make more efficient the CISIApro engine implementing different algorithmic optimizations. But the last important improving introduces a new **Spatial Propagation** in the already complex CISIApro engine simulation (see Figure 3.13).

Introduction of a *Spatial Propagation* means to have, in addition to the already well-known deterministic propagation, a propagation directly correlated to spatial geometries which could be defined in a model. Through a new module it is possible to:

- Define an '***Event***' with its *Spatial Epicentre*;
- Declare the ***Spatial Variables*** (e.g.: $x, y, z, lat, long, \cdots$) which can identify an entity in a specific space;
- Define the initial ***Magnitude*** (M);
- Define the ***Distance*** (D) in function of the *Spatial Variables*

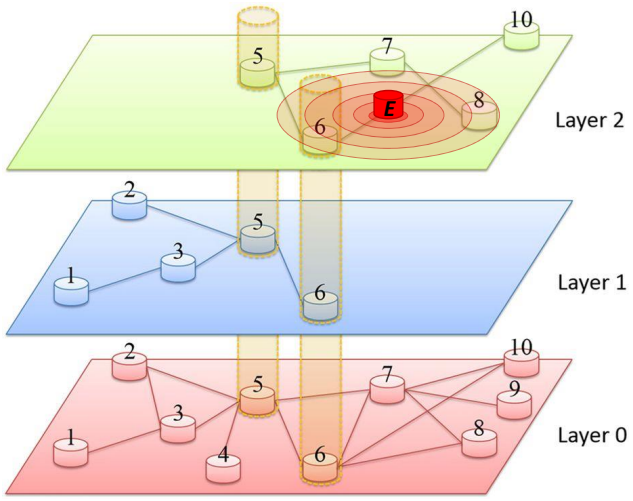


Figure 3.13 Spatial Event Propagation in a Multidimensional Graph.

$$D = f(SpatialVariables);$$

- Define the ***Propagation*** (σ) effect in function of the given *Distance*, *Magnitude* and *time*

$$\sigma = f(D, M, t);$$

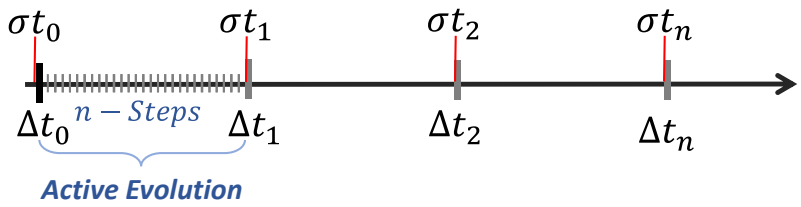


Figure 3.14 Entity time-line steps evolution with a spatial propagation.

Also in this type of propagation it is possible to define, or not, a correlation with the time in order to have a dynamic or instant spatial propagation effect into the simulation.

Chapter 4

Dynamic Risk Analysis in a Cyber Context

Dependencies and interdependencies between critical infrastructures are difficult to identify and model because their effects appear infrequently with unpredictable consequences. Telecommunication networks based on commonplace technologies (such as Ethernet) often constitute a vulnerable attack vector against modern Critical Infrastructures (CIs), particularly for Supervisory Control and Data Acquisition (SCADA) systems, which rely on them for monitoring and controlling physical components.

The addition of cyber attacks in this context makes the analysis even more complex. Integrating the consequences of cyber attacks and interdependencies requires detailed knowledge about both concepts at a common level of abstraction. CISIApro, as critical infrastructure simulator, was created to evaluate the consequences of faults and failures in interdependent infrastructures. This chapter demonstrates the use of CISIApro to evaluate the effects of cyber attacks on physical equipment and infrastructure services. A complex environment involving three interconnected infrastructures is considered: a medium voltage power grid managed by a control center over a SCADA network that is interconnected with a general-purpose telecommunications network. The functionality

of the simulator is showcased by subjecting the interconnected infrastructures to an ARP spoofing attack and worm infection. The simulation demonstrates the utility of CISIApro in supporting decision making by electric grid operators, in particular, helping choose between alternative fault isolation and system restoration procedures.

This architecture solution has been tested on a hybrid environment testbed, made of virtual and real components, within the scope of the EU FP7 CockpitCI. The case study corresponds to a medium voltage power grid controlled by a SCADA control center, where the platform has been validated with optimal results in terms of detection capabilities and time response.

4.1 Introduction

Critical Infrastructures (CIs) are vital for our lives: airports, rail transport, network communications, electricity grid, oil refineries and water systems are some examples of those key-assets. Industry and infrastructure owners uses the so-called "N-1" standard, referring to the ability to operate without the loss of service even after the failure of one key component. The industry achieved the capability to operate also with the loss of two key component ($N-2$). In Critical Infrastructures, also the "$N-2$" standard, is not enough: a major service outage, a possible coordinated cyber threat or faults started in other interconnected infrastructures must be considered and evaluated in order to restore the service as soon as possible.

During the last fifteen years, researchers are faced with the problem of interdependencies, how to model it and how to early detect the cascading effects of failures in a single infrastructure. The most famous example of vulnerable infrastructure was in 2003 the North-America electrical grid blackout. This blackout was due to a software bug in the control room causing effects on water supply, transportation, communication systems and industries [32]. Other possible case studies are natural disaster such as

hurricane Katrine: the storm interrupted oil production, importation and refining, involved ocean shipping and exports and impacted severely the local electric utility [33].

Critical infrastructures adhere to the "$N-1$" standard and they are protected from failures that initiate in their own sectors. In the event of a failure in the power grid, operators can reconfigure the grid to isolate the fault and restore power to customers (some users might still not have power, but the blackout is not complete). The reconfiguration procedure can be automated or executed manually and it depends on the specific topology (the sequence of opening and closing circuit breakers is related to the topology) as well as on other infrastructures, especially the telecommunications network, which is used to send commands to circuit breakers. This procedure is called fault isolation and system restoration (FISR) or power load shedding.

If a cyber event or a failure occurs in the telecommunications network, the procedure for restoring power may fail without any alerts being sent to power grid operators. In this situation, a routine failure can evolve to become a large-scale blackout that lasts for an extended period of time. One of the most famous cyber attacks on a SCADA network was perpetrated by Stuxnet [34]. This chapter focuses on the modeling and assessment of the impacts of cyber events on interconnected critical infrastructures.

The wide spread of telecommunication networks leads to unknown and dangerous situations that can have uncontrolled effect on physical equipment of Critical Infrastructures. The problem of how to detect cyber anomalies is outside the scope of this paper. We can assume that an IDS (Intrusion Detection System) or a malware protection send the data flow related to anomalies.

The vast reach of telecommunications networks leads to poorly understood situations that can have uncontrolled effects on physical equipment in critical infrastructure assets. However, the problem of detecting cyber anomalies is outside the scope of this research because the approach presented here is independent of anomaly detection

techniques. Indeed, the assumption here is that intrusion detection systems and malware protection software are in place to collect data about potential anomalies. This chapter demonstrates the application of CISIApro to evaluate the effects of cyber attacks on physical equipment and infrastructure services. A complex environment involving three interconnected infrastructures is considered: a medium voltage power grid managed by a control center over a SCADA network that is interconnected with a general-purpose telecommunications network. The functionality of the simulator is illustrated by subjecting the interconnected infrastructures to an ARP spoofing attack to compromise a secure communications channel, which is then used to launch a worm infection. The simulation demonstrates the utility of CISIApro in supporting decision making by electric operators, specifically helping choose between alternative fault isolation and system restoration procedures.

4.2 Cyber Attack Impact Assessment

Motivated by Stuxnet, researchers have focused on understanding how cyber attacks can affect physical critical infrastructure assets by leveraging SCADA telecommunications networks. This problem is complex because it requires deep knowledge from different domains – telecommunications and the specific physical infrastructure. Smart grids and power grids, in general, are perfect environments for evaluating the effects of cyber threats. Power grids have detailed analytic models at almost every level of abstraction and they also have well-documented control algorithms.

Lemay et al. [35] have used an industrial control system sandbox for the cyber portion of a cyber-physical system and optimal power flow algorithms for an electrical simulator to replicate the physical portion of an electrical power grid. The ability to model the physical damage caused by cyber attacks enables defenders to accurately evaluate the risk using metrics such as the delivered power and generation costs.

Sgouras et al. [36] have analyzed the impact of denial-of-service and distributed denial-of-service attacks on a smart meter infrastructure. They demonstrated that an attack on a single meter causes a temporary isolation or malfunction, but does not impact the power grid. However, the partial nonavailability of the demand-response mechanisms in a large number of smart meters due to a distributed denial-of-service attack could impact load shedding when the grid reaches an unsafe zone close to its maximum capacity. For these reasons, an attacker would prefer to conduct a distributed denial-of-service attack during a peak-use period in order to achieve greater impact.

Dondossola et al. [37] have assessed the impact of malware using a cyberphysical risk index that incorporates a probabilistic interpretation of vulnerability existence, threat occurrence and intrusion success. The basic idea underlying the cyber assessment methodology is to adopt a frequency interpretation of probability; specifically, the probabilities comprising the risk index are translated to their corresponding frequencies.

Another approach is to fuse information from the cyber and physical domains. To accomplish this, Santini et al. [38] have developed a data fusion framework using evidence theory. The data fusion framework was used to identify the cause of a cyber-physical attack (i.e., a denial-of-service attack that caused a breaker in a smart grid to malfunction).

Critical infrastructure operators are especially interested in the quality of the the services provided to their customers. Therefore, it is vital to understand the effects of cyber attacks on physical systems and their services. The CISIApro simulator used in this research is specifically designed to help determine the consequences of cyber attacks on physical equipment and the services they provide.

4.3 Proposed Architecture

As illustrated in Figure 4.1 the physical system data is gathered from the SCADA control center and the cyber threat data is obtained from cyber detection systems such as Intrusion Detection System (IDS) and anti-virus software. All the information is translated (normalized) and saved into the CISIApro database as well as the propagation results are placed in a secondary CISIApro output database structure after each CISIApro simulation engine run (called also CISIArun). The CISIApro execution results and decision support information are displayed to operators via human-machine interfaces (HMIs).

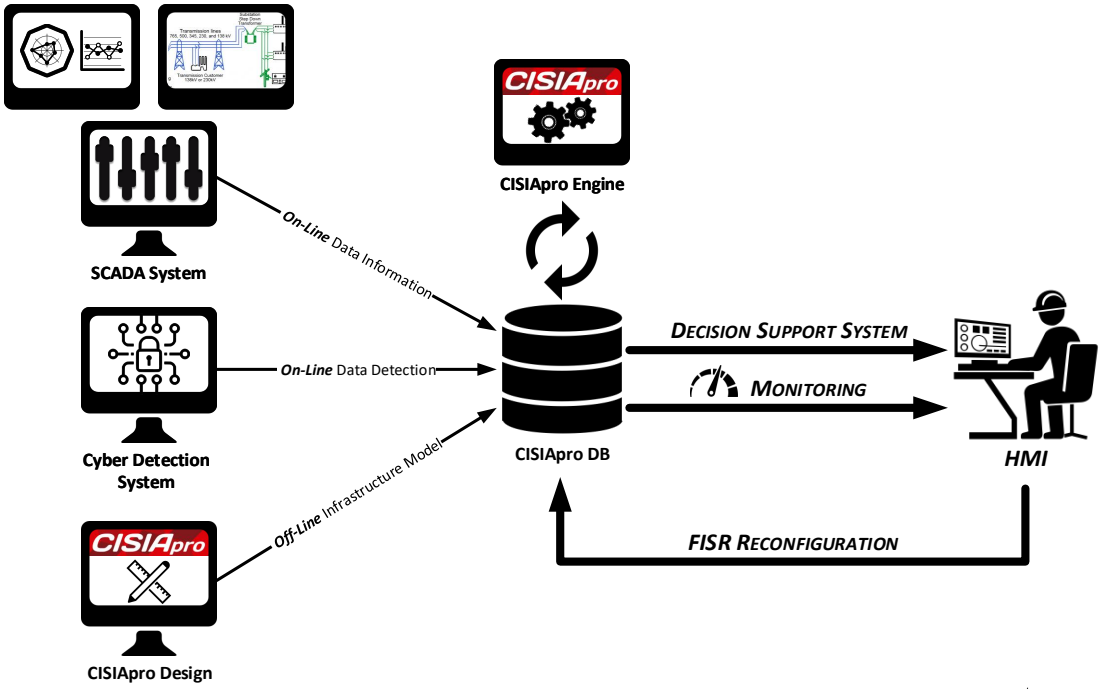


Figure 4.1 Proposed architecture.

4.4 Case Study

The case study considers three interconnected infrastructures: a medium voltage power grid controlled by a SCADA network and connected to a general-purpose telecommunications network. Interested readers are referred to [39] for details about the interconnected infrastructures.

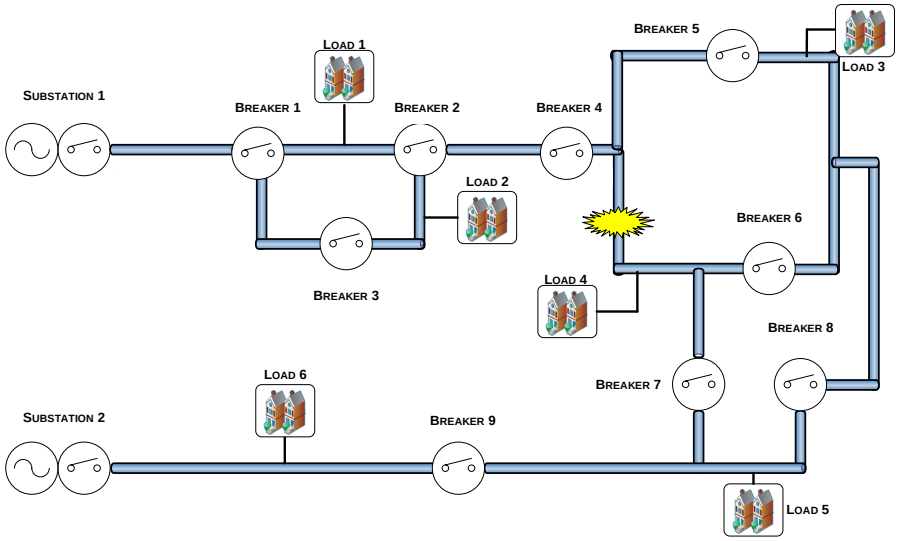


Figure 4.2 Medium Voltage Power Grid.

Figure 4.2 shows a portion of the medium voltage power grid. It consists of two lines fed by two substations that transform current from the high voltage grid. During normal conditions, the two lines are usually disconnected by two circuit breakers that are normally open (Breakers no.7 and no.8 in Figure 4.2). Also, Breakers no.3 and no.5 are open in order to maintain a radial topology.

All the circuit breakers, except for the two located at the substations (not numbered in Figure 4.2), are controlled from the SCADA control center via a telecommunications network. This proprietary network, which belongs to the power grid owner, uses a protocol compatible with TCP/IP. A remote terminal unit (RTU) is directly connected

to each circuit breaker, except for the two breakers located at the substations. The SCADA control center in Figure 4.3 sends commands to the remote terminal units to open or close the associated circuit breakers.

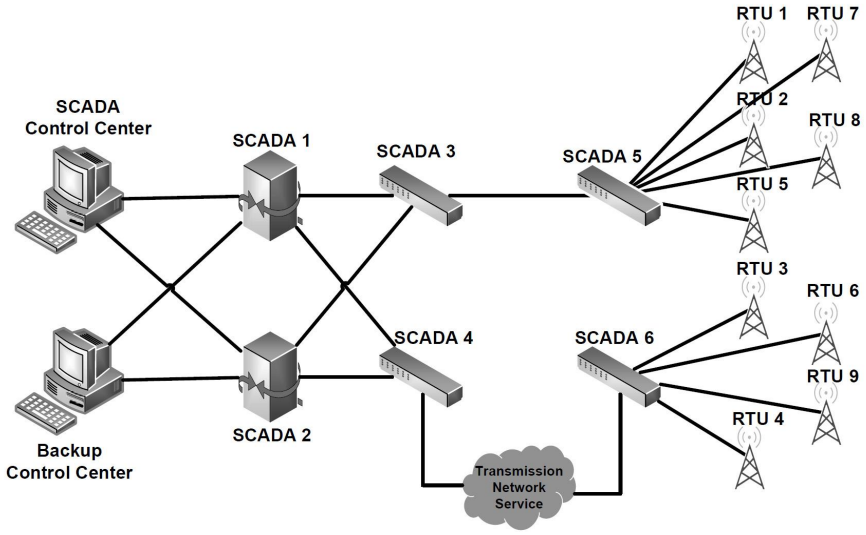


Figure 4.3 SCADA Control Center.

Figure 4.4 shows the general-purpose telecommunications network (i.e., Internet) that is connected to the SCADA system. The network essentially has a ring topology. In the event of a link failure, network packets are transmitted back to the sending node in order to change the routing protocol.

In the case of a permanent failure in the power grid, the operator executes a fault isolation and system restoration procedure to open or close circuit breakers. This procedure determines where the fault occurred and how to restore power to customers after the damage is repaired. If a cyber fault occurs in the telecommunications network, then the fault isolation and system restoration procedure fails with unpredictable consequences.

The attack scenario considered in this work involves a cyber attacker who attempts to modify the behaviour of the power grid using a computer worm to infect the remote

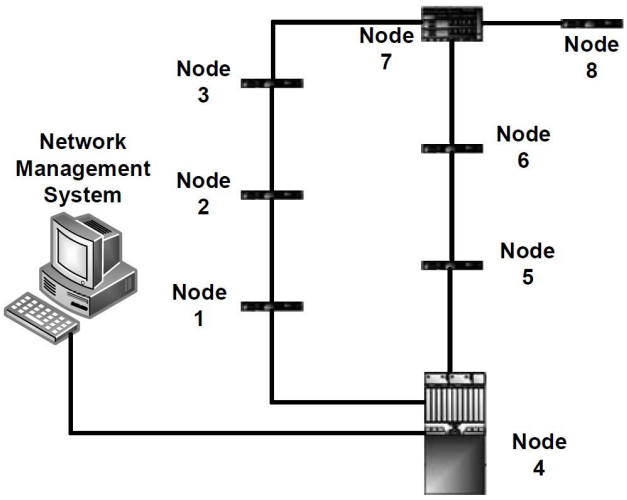


Figure 4.4 Telecommunications Network.

terminal units, as in the case of Stuxnet [9]. The attack begins with an ARP spoofing attack that exploits ARP vulnerabilities. The goal is to map the attacker's MAC address to the IP address of a trusted node in the network so that traffic directed at the trusted node is sent to the attacker. The attacker is assumed to be connected to the telecommunications network and uses the connectivity to send the worm to the remote terminal units and their associated circuit breakers.

4.5 Results

In order to properly demonstrate the ability of CISIApro, we depicted the results of the experiment (Figure 4.5), which lasted 40 seconds in a real scenario validation and which is divided in two parts.

The first part, lasting from seconds 1 to 10, involves the attacker performing a man-in-the-middle attack on the SCADA network, (Figure 4.3) as described on previous sections. The second part, lasting from seconds 11 to 40, involves an infection being spread from the attacker in the aftermath of the MITM attack.

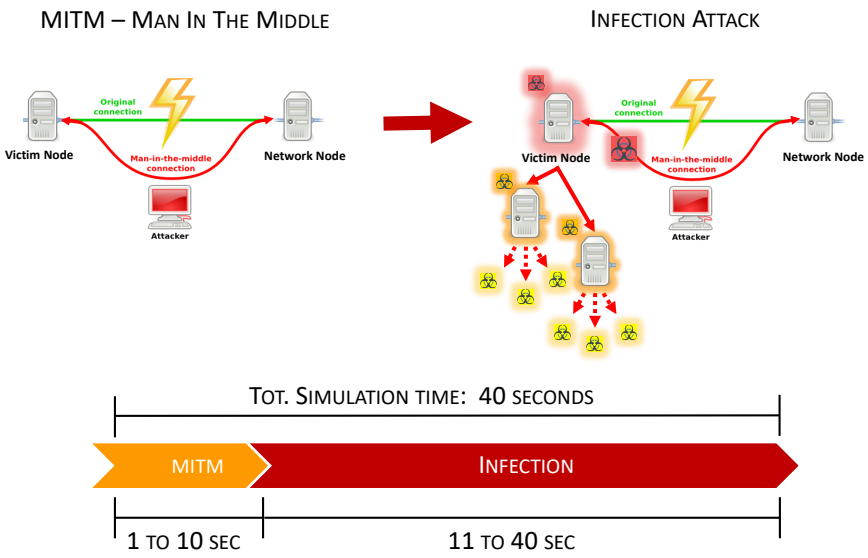


Figure 4.5 Experimented cyber attack scenario.

The man-in-the-middle attack has a static aspect – no changes occur during the first 10 seconds of the simulation for the involved entities. During the malware spreading, the ability to properly telecontrol power switches is downgraded and can not be guaranteed.

For the MITM attack, the spreading rule is related to the distance of the infected node: the greater is the number of hops needed for reach the node, the lower are the effects of the cyber attack and the risk of node malfunction. Simulation results show that Telecommunications Node no.6 (Figure 4.4) operational level was 0.4 during the man-in-the-middle attack. The operational level of the downstream SCADA node (Node no.6 in Figure 4.3) was 0.85. The operational levels of the remote terminal units connected to SCADA Node no.6 (in particular, RTUs no.3, no.4, no.6 and no.9 on Figure 4.6) were also 0.92.

For the malware spreading, the propagation is still related to the distance, but each node has an increasing exponential trend for the effect of the malware. The exponential function and its parameters have been obtained starting from literature reviews, expert

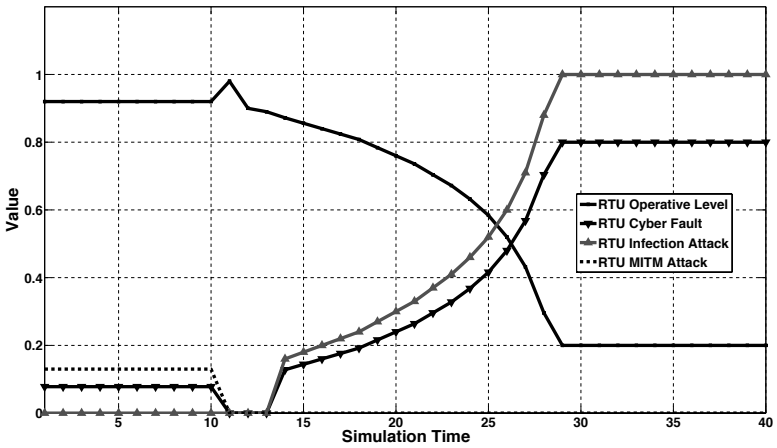


Figure 4.6 Operational level of a subset of PLCs (numbers 3, 4, 6, 9)

interviews, historical data (if existing) and from some simulations, and then extracting the best fitting pattern from all available information.

When the malware is detected at 11 seconds, the SCADA telecommunication node is highly affected and the information has a high trustworthiness, see Figure 4.7.

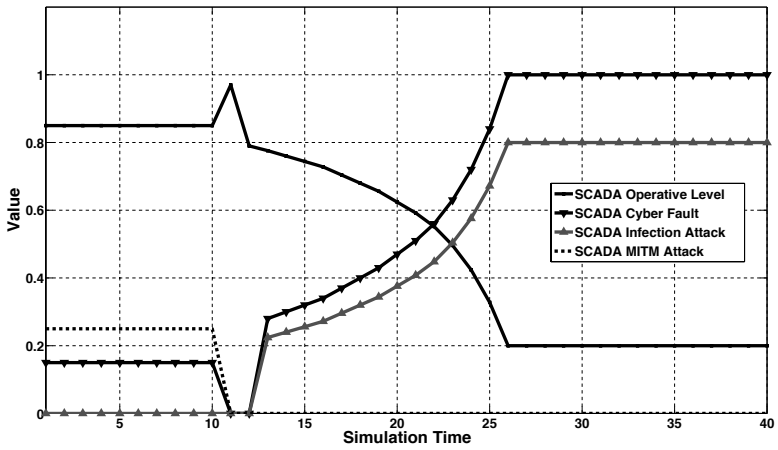


Figure 4.7 Operational level of SCADA node number 6

The trends of the entities are related to the distance and therefore the node needs more time to become completely unavailable. The set of PLCs (number 3, 4, 6, and 9 in Figure 4.3) linked to the SCADA node no. 6 has a similar trend of the up-stream node with a delay of one time step, see Figure 4.6.

The main aim of the CISIApro simulator is to help the decision making of the operator. The reconfiguration procedure of an electrical grid is a very easy and common task for the operator, but requires interconnected infrastructures. Supposing a fault in the power grid, depicted in Figure 4.2 as a yellow explosion, two alternative configuration are considered:

- **FISR no. 1** - opening breakers no. 4 and no. 6; breakers no. 7 and no. 5 are already open; the only disconnected customer is number 4; load number 3 is fed from the substation no. 2;
- **FISR no. 2** - opening breakers no. 4 and no.6; customers no. 4 and no. 3 are isolated.

The two reconfiguration procedures are affected differently due to infection spreading: the first FISR is less risky than the second one because involves PLCs that are not affected by the malware. Therefore, the platform is able to suggest the less-risky reconfiguration option, in order to improve electrical operator readiness in case of cyber attacks, where quick response time is mandatory.

4.6 Conclusions

The simulator helps evaluate the impacts of cyber attacks on interdependent infrastructures; the attacks include ARP spoofing, SYN flooding and worminfections. CISIApro has been validated using complex case studies involving approximately 70 entities (Figure 4.8) that exchange around twelve distinct resources. The case study described in this chapter involves three interconnected infrastructures: a medium voltage power grid managed by a control center over a SCADA network that is interconnected with a general-purpose telecommunications network. The real-time simulation involving an ARP spoofing attack and worm infection demonstrates the utility of the CISIApro for

supporting decision making by electric grid operators, in particular, helping choose between alternative fault isolation and system restoration procedures to reduce the attack impact and enhance system recovery.

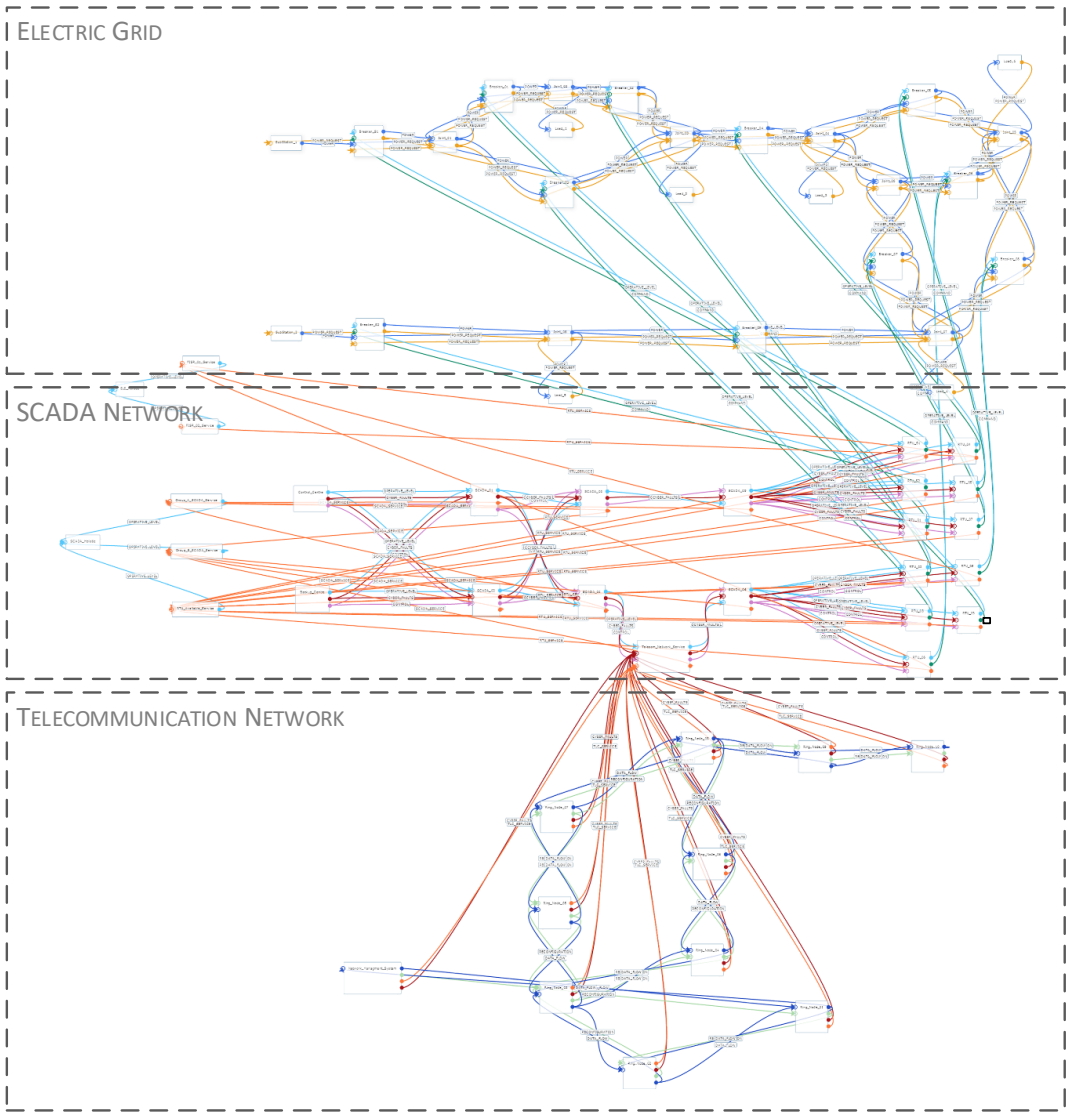


Figure 4.8 CISIApro CockpitCI model.

Chapter 5

Dynamic Risk Analysis for Disaster Recovery

In the last ten years, the emergency response has been a key point for the welfare of citizens as well as for the economic losses. The widespread technology deployment improves the emergency response but the existing interdependencies among physical and cyber systems generate unpredictable consequences in the reconfiguration procedures. The European project URANIUM aims to provide a timely and an efficient tool for decision support that is simple to use also in complex emergency scenarios. This system gathers data from several SCADA (Supervisory Control and Data Acquisition) systems of Critical Infrastructures (CIs), such as power grid, gas and pipelines, telecommunication network, and transportation. The core of URANIUM project is two cascading modules: the first is CISIApro tool for evaluating risk of interdependent CIs and the second is an expert system for managing civil protection operations. CISIApro tool fuses data and information coming from SCADA systems in order to understand the consequences of negative events, such as faults, natural disasters and cyber-attacks. CISIApro models infrastructures and their interdependencies using an agent-based technique where each agent evaluates its own risk using information coming from its neighbourhood. The

expert system is based on structured decision support methodologies. It provides a suggestion for managing and optimizing the intervention procedures of civil protection. The output of this process is a cockpit, i.e., a synoptic view of predicted situations and a suggestion for emergency procedures.

The decision support systems are based upon the output of CISIApro tool, an agent-based simulator for evaluating risk of interdependent systems. This tool has been applied within the European URANIUM CIPS project by means of a realistic and quite complex reference scenario made of four interconnected infrastructures in a regional area. System output is visualized through a synoptic web-based view of predicted situations and suggested procedures. The results have been validated by means of national and international stakeholders, such as Italian Civil Protection operators and electrical operators.

5.1 Introduction

Modern societies are highly dependent on the continuous operations of their critical infrastructures that deliver critical goods and services. These include electricity, drinking water, information and communication technologies and waste disposal. Interruptions can have repercussions on the population and may affect other critical infrastructure through the domino effect: for example, a large power outage will affect immediately drinking water supply, telecommunications and rail. The European security as well as the quality of life of its citizenry depends on the continuous reliable operation of a collection of complicated interdependent infrastructures including transportation, electric power, oil, gas, telecommunications and emergency services. A disruption in one infrastructure can quickly and significantly impact another one, causing ripples across the nations. The importance of critical infrastructure is also clear from the fact that they can be defined as those industrial capabilities, services and facilities that

in case of interruption of their normal operation can affect people's lives and, most important, can damage or destroy people's lives. During last decades, infrastructures are increasingly reliant on new information technologies, that allow for enormous gains in efficiency but they also create new vulnerabilities against natural disasters or terrorist attacks. Among international organizations critical infrastructure protection concerns, NATO was the first to be involved in this field. In 2009, NATO issued a series of definitions in the field, supported by all Member States and partner:

- critical infrastructure are those facilities, services and systems that are so vital to the nation, that their removal from service or destruction is potentially destabilizing national security, economy, health of the population and the effective functioning of government;
- CIP includes programs, activities and actions taken by governments, owners, operators and shareholders to protect these infrastructures.

Senior Civil Emergency Planning Committee within NATO has notified the eight subordinate committees to find solutions as an integrated approach to issues such as criteria for determining critical infrastructure, risk analysis methods and identifying vulnerabilities and their methods of protection. In particular, there are different forms of natural disasters, as typhoon, heavy rains, sea level rise, flooding, earthquake, etc. These natural disasters have caused significant economic, social, financial, property, environmental degradations, infrastructure damages and also tragic loss of human lives.

When an emergency occurs, the relevant management personnel or decision-makers (DMs) need to decide what actions to take instantly to mitigate or minimize the negative effects. Such catastrophic incident reveals the need for efficient planning and the need for careful decision to be taken during the first few minutes following an incident. Decisions are critical to successful mitigation, damage management, death prevention,

injury, structural loss, and the overall solution of the crisis. Project URANIUM consists of an intelligent decision making system that optimizes the allocation of resources following an infrastructure disruption and suggests how the resources could be utilized during disaster response. It provides a timely and an efficient tool for decision support that is simple to use also in complex emergency scenarios.

5.2 Contributions

This work take into account how natural disasters can affect a set of four interconnected critical infrastructures within a regional area. It is described the complete information flow from sensor data coming from the field to the decision support systems. The main aim of this process is to demonstrate how one critical infrastructure interdependencies simulator (i.e., CISIApro) can be used for different aims. The contribution of this work is three-fold:

1. provides the overall process for evaluating the consequences of adverse events on a complex reference scenario and for making better decisions. This process is made of CISIApro simulator for understanding the effects of faults and natural disaster on equipment and services of the infrastructures, by means of a risk metric. The key process regards emergency response activity of the civil protection where telecommunications and rail-roads are needed for first interventions.

2. performs the data exchange among the critical infrastructure control centres by means of a common simulator able to fuse information. CISIApro simulator is able to define an inner risk metric (i.e., the operative level) for each agent within the simulator and send those data to the decision support systems.

3. demonstrates how smart decision making systems must be used during disaster response optimizing the allocation of resources during the restoration process.

The resulting system provides a timely and an efficient tool for decision support that is simple to use also in complex emergency scenarios.

5.3 Decision Support Systems in Emergency Management

Interdependencies between critical infrastructures are increasing dramatically as a result of the pervasive use of information and communications technologies. The interdependencies create opportunities, but they also induce vulnerabilities. Exploitation of these vulnerabilities produces negative impacts that are becoming more frequent, longer-lasting and more widespread. A systematic method for evaluating interdependencies and the outcomes of adverse events is needed to mitigate and manage the risk to critical infrastructure assets [40].

Considerable research has focused on decision analysis and support for emergency response operations. Various decision making methods have been proposed for natural events such as floods, fires and industrial hazards. Decision support systems for reducing flood damage are presented in [41, 42]. A multi-criteria evaluation method and a multi-attribute risk analysis method for nuclear accidents are described in [43, 44], respectively. A decision support system for risk analysis and impact evaluation of crisis scenarios involving critical infrastructures is presented in [45]. This research builds on previous work by leveraging the results of an infrastructure interdependency model to enhance decision making during emergency situations.

Several researchers have applied multi-criteria decision making techniques to emergency management. Peng et al. [46] have proposed an incident information management framework based on data integration, data mining and multi-criteria decision making. Ergu et al. [47] have developed a simple consistency test process to solve decision

making problems in emergency situations. Hwang and Yoon [48] have specified a technique for ordering preferences based on their similarity to the ideal solution using multi-criteria decision making.

Analysis of the literature reveals that little research focuses specifically on decision support systems for civil protection control room personnel. Moreover, no approach uses the ELECTRE II method [49]. The ELECTRE II method is appealing because it strikes a balance between the amount of data processed and the computational time. However, the method is not good enough to assign interventions in civil protection scenarios. Therefore, this research has focused on the development of a tool that leverages a more complex variant of the greedy algorithm of Martello and Toth [50] to solve the knapsack problem and assign appropriate interventions.

5.4 Proposed Architecture

Basically, proposed architecture (Figure 5.1) consists of two cascading modules: the first is CISIApro tool for evaluating risk of interdependent Critical Infrastructures (CIs) and the second is an expert system for managing Civil Protection operations. CISIApro tool fuses data and information coming from SCADA systems in order to understand the consequences of negative events, and models infrastructures and their interdependencies using an agent-based technique where each agent evaluates its own risk using information coming from its neighbourhood. The expert system is based on structured decision support methodologies. It provides a suggestion for managing and optimizing the intervention procedures using a hybrid algorithm involving multi-criteria decision making and a knapsack algorithm. The multi-criteria decision making technique sorts the interventions based on a set of criteria while the knapsack algorithm assigns each intervention to a civil protection district.

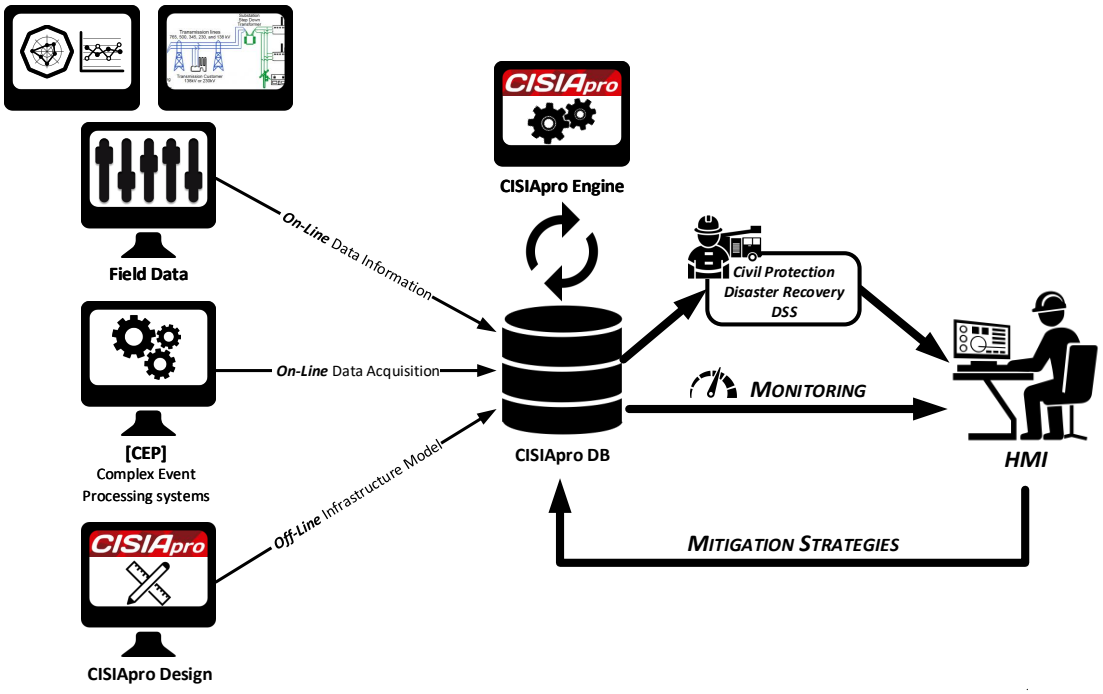


Figure 5.1 Proposed architecture.

5.5 Decision Support System Implementation

The decision support modules consider a protection level and an event propagation level:

- **Protection Level**: This level expresses the ability of each zone to counter emergencies. The protection level assumes a value from zero to one, where zero means that no operational resources are available and one means that all the resources are available. The protection level corresponds to a mitigation action that is applied after a catastrophic event occurs.

- **Event Propagation Level**: This level expresses the propagation of an adverse event in the neighborhood due to geographical proximity and to specific features (e.g., wind direction in the case of a fire). The event propagation level assumes a value from zero to one, where zero means that no adverse event will occur in the

near future (i.e., 5-10 minutes from the first alert) and one means that a disaster is a certainty.

The protection and event propagation levels are discretized into five stages:

(i) normality;

(ii) attention;

(iii) early warning;

(iv) warning;

(v) emergency.

Therefore, proper threshold values must be introduced in order to determine the actual states. First, an emergency situation is defined in terms of civil protection operations. This is accomplished by implementing a numerical comparison to identify the alert level in each area and for each type of event; specifically, the propagation level is compared against a pre-set alarm threshold value. The actual propagation level is evaluated by CISIApro by considering an event v and the geographic area i, which usually corresponds to a town. The outputs of this phase are the type and level of warning for each city i, which are obtained by comparing four different thresholds for event v:

(i) attention threshold value S_v^N;

(ii) early warning threshold value S_v^P;

(iii) warning threshold value S_v^A;

(iv) emergency threshold value S_v^E.

Next, the CISIApro results are used to determine the alarms that are related to large disasters and those that are due to single mechanical faults. This phase, which is

similar to the previous phase, performs numeric comparisons between the operative levels and pre-defined thresholds S^N, S^P, S^A and S^E.

A multi-criteria decision making method of the ELECTRE II family is employed to identify one or more solutions that best meet the requirements (criteria), Consider a situation where a decision maker is presented with n alternatives and m criteria or attributes, where the alternatives A_1,A_2,...,A_n are explicitly listed and an attribute is assigned to each alternative/criterion.

A decision matrix assigns values to the alternatives according to the criteria, where a matrix element e_{ij} corresponds to the alternative A_i scored according to criterion j. The decision maker also assigns a *weight* w_j that expresses the relative importance of criterion j with respect to the other criteria.

Two types of analyses enable the verification of the relative ranking of two alternatives:

(i) concordance analysis, which considers the factors and criteria that do not present negative evidence that one alternative is preferred over another;

(ii) discordance analysis, which considers the negative evidence in choosing one alternative over another.

An important concept in this work is the notion of *preference* (P_j). Given two alternatives A_h and A_k, A_h is preferable to A_k (denoted as $A_h\ P_j\ A_k$) according to the j criterion if $e_{hj} \geq e_{kj}$. In other words, A_h is preferable to A_k if there is great satisfaction in preferring A_h to A_k and there is no great in-satisfaction in preferring A_h to A_k.

Thus, given two alternatives A_h and A_k, A_h dominates A_k ($A_h \geq A_k$) if $e_{hj} \geq e_{kj}$ for each $j = 1, \ldots, m$. If A_h is preferable to A_k, it means that A_k is dominated by A_h.

The *ELECTRE II* procedure defines a concordance value c_{hk} and a discordance value d_{hk}, for each couple (A_h, A_k), $h \neq k$, as generic elements of the concordance

matrix C and discordance matrix D, respectively. The concordance value takes into consideration the weight of the criteria according to which h is preferable to k

$$c_{hk} = \frac{\sum_{j:A_h P_j A_k} w_j}{\sum_j w_j} \tag{5.1}$$

where $h = 1, \ldots, n, k = 1, \ldots, n, j = 1, \ldots, m$.

The discordance value takes into consideration the criteria opposing to the preference of h to k:

$$d_{hk} = \max_{j:A_k P_j A_h} \left\{ \frac{e_{k_j} - e_{h_j}}{diffMax_j} \right\}, \qquad diffMax_j = \max_j \left\{ e_{h_j} - e_{k_j} \right\} \tag{5.2}$$

where $h = 1, \ldots, n, k = 1, \ldots, nandn, j = 1, \ldots, m$.

ELECTRE II introduces two veto thresholds, strong f and weak d, to assess the outranking alternatives. Note that one alternative outranks another if it outperforms the other alternative for a sufficient number of criteria and is not outperformed by the other alternative (in the sense of having significantly inferior performance) for any criterion.

Also, ELECTRE II introduces two concordance thresholds such that $0 < S_C^d < S_C^f < 1$; if both concordance thresholds tend towards one, then there exists one concordance only and no conflict choosing one alternative over the other. Additionally, it introduces two discordance thresholds such that $0 < S_D^f < S_D^d < 1$; if both discordance thresholds tend towards one, then no regret exists in choosing one alternative over the other. Therefore two outranking relations exist:

- **Weak outranking**: $A_h S_D A_k$ if and only if $c(h,k) \geq S_C^d$ & $d(h,k) \leq S_D^d$
- **Strong outranking**: $A_h S_F A_k$ if and only if $c(h,k) \geq S_C^f$ & $d(h,k) \leq S_D^f$

Thus, two graphs are obtained, one weak and one strong, which enhance the level of available information and make the choices more accurate. The strong graph is more rigid and strict with few out-rankings and many non-comparabilities (i.e., difficult to compare due to missing information during the time of evaluation). The weak graph is less restrictive and richer in out-rankings and presents fewer non-comparabilities. The classification of the final alternatives is obtained using two differently-ordered algorithms, one ascending and one descending.

The multi-criteria decision making technique does not consider resource allocation for each civil protection district. For this reason, a modification of the knapsack problem is implemented using a heuristic approach. This method compares the total propagation level d_i of abnormal events detected in city i with the protection level LP_g of the nearest district g ordered according to the results of the previous phase. If a positive result $LP_g - d_i \geq 0$ is obtained, then the intervention is assigned to district g because the district has enough resources. Otherwise, if $LP_g - d_i < 0$, then the algorithm assigns the intervention partially to district g for the available resources, and the remaining to another district based on its proximity and the estimated arrival time. The estimated arrival time t_{ig} is computed as:

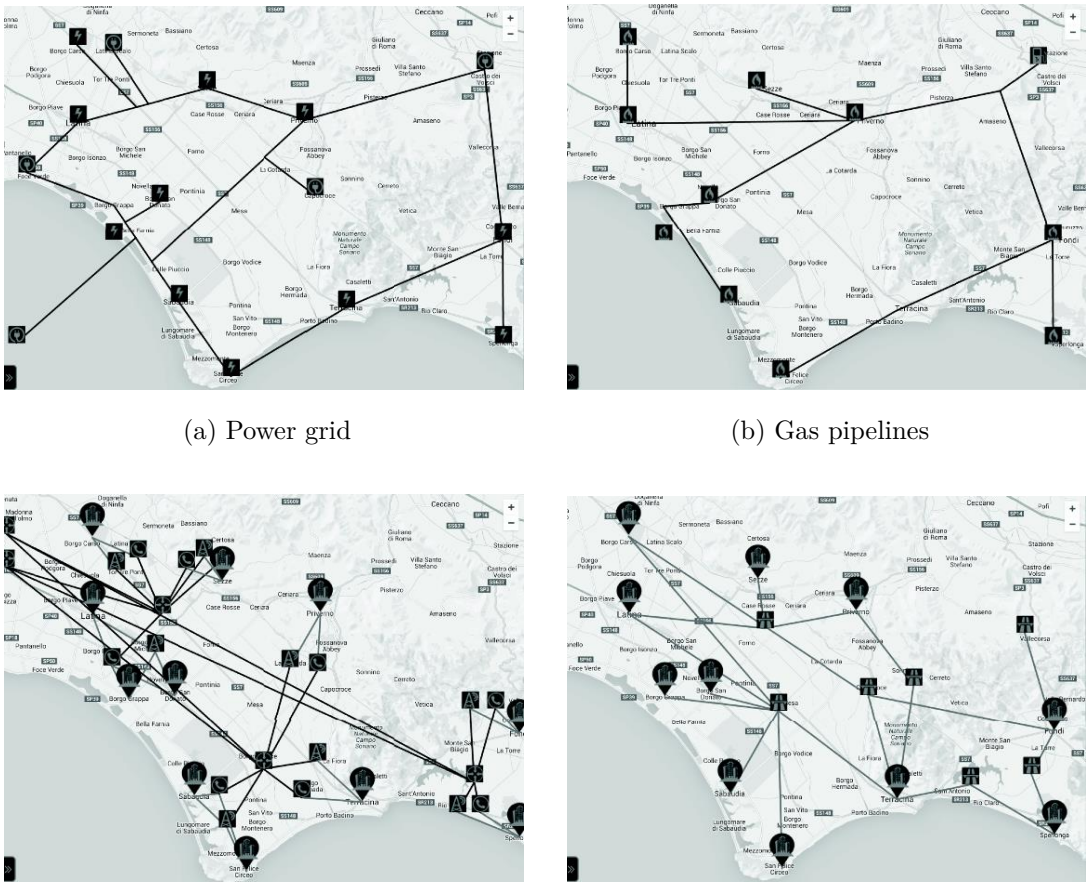
$$t_{ig} = dist_{ig}(2 - LV_{iq}) \tag{5.3}$$

where $dist_{ig}$ is the distance between the city i and the district g and LV_{ig} is the operative level of the roads between the city and the district, coming out from CISIApro results.

If the combined actions involving different districts are unable to address the emergency, then the decision support system advises the emergency management room operator that the available resources are insufficient and an intervention by external forces is required.

5.6 Case Study

The reference scenario of this work is made of four interconnected critical infrastructures: a medium-voltage power grid with its SCADA control center, a gas distribution network with its control center, a telecommunication network and the transportation roads, see Figure 5.2. The Prefecture's historical documents suggest us some possible adverse events that we can consider within the reference scenario. Possible natural events are earthquakes, adverse climatic events, forest fires, hydro-geological events and industrial hazards.



(a) Power grid

(b) Gas pipelines

(c) Telecommunication networks

(d) Road system

Figure 5.2 Reference scenario using the layers of CISIApro GIS.

In Figure 5.2a, the power grid has a mesh topology and is fed from the power transmission network by means of two primary substations with transformers. The power grid has also an off-shore wind farm, a solar farm and a natural-gas power plant. The topology of the electrical grid is take into account in event of permanent faults. Electrical operators are able to reconfigure the topology through opening or closing circuit breakers, in order to isolate the fault and restore the power to customers.

The distribution gas pipelines have a radial topology from the regulator connected to the gas transmission network in Figure 5.2b. The model considers a set of pumping stations maintain constant the gas pressure by means of compressors. If a leakage happens or if a compressor is out of order, the storage supplies the gas pipelines to fed customers. The natural gas is also used as fuel for electric generators connected to circuit breakers, but it also used as input for the natural-gas power plant. Electricity is needed for pumping stations and regulators within the gas pipelines.

Both those two infrastructures have a SCADA control center, not depicted in Figure 5.2, able to collect data from sensors and change pre-defined threshold or values for generators. Those SCADA control center make use of an Ethernet-based telecommunication network.

The telecommunication network is depicted in Figure 5.2c and it has a mesh structure and is made of optical fiber. We model it for land-line and mobile services, for understanding how coordinate crises. Telecommunication network is actually used among electric and gas SCADA control center and field sensors. Telecommunication routers and switches need electricity to proper work.

Another relevant sector for URANIUM project (Figure 5.4) is the transportation one, see Figure 5.2d. During emergencies, it is mandatory to provide for both residents and responders the access at the evaluation routes. The first responders include police forces, fire-fighters, coast guards and hospital volunteers. The ground transportation system is

Figure 5.3 Reference scenario main cities, representing eleven areas.

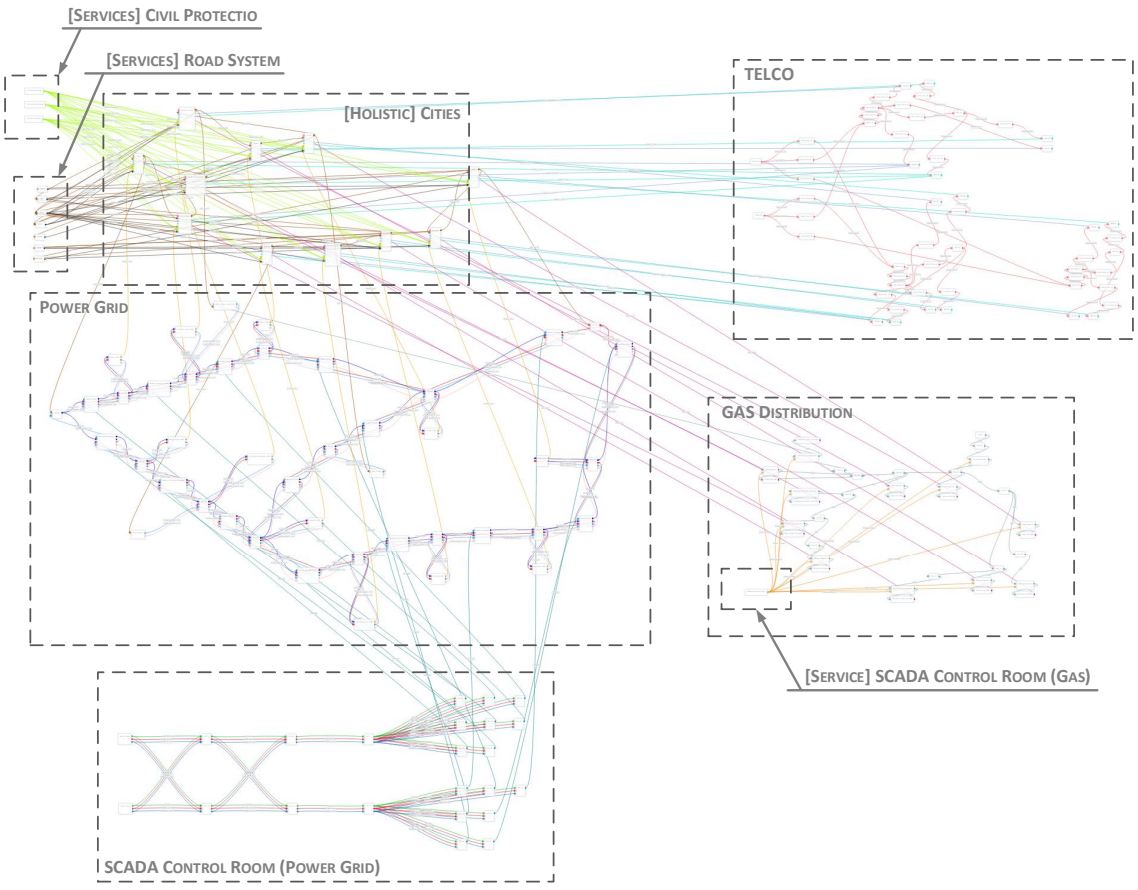


Figure 5.4 CISIApro URANIUM model.

the main focus within our reference scenario. Within the ground transportation system, we model several principal and secondary routes to connect cities of the reference scenario. Our main focus in that field is the ground transportation system. In an emergency case it is mandatory to provide for both resident and emergency responders the access at the evacuation routes. During emergencies, Civil Protection is in charge of the protection of the citizens. Several actors play crucial roles in the Civil Protection countermeasures: police force, fire-fighters, coast guards, hospital volunteers. Each of these actors provides their means for the welfare of the people. Hence for the ground transportation system, our modelling choice has been the identification of several principal and secondary routes to connect cities of the rural area.

5.7 Results

After several days of rain, water release from a dam on the Amaseno river causes the operative level of the city of Priverno to decrease to 0.35 (according to the CISIApro model). The flooding affects the area closest to the dam due to the dense irrigation canal network in the Pontine levee, potentially causing the levee to collapse. The interdependency model reflects this situation and reduces the operative level to 0.675 for the cities of Sezze, Cisterna di Latina, Latina, Borgo Grappa, Borgo San Donato, Sabaudia and San Felice Circeo (Figure 5.3).

Figure 5.5 shows the decreased operative levels of the cities resulting from downgrades of the connected infrastructures (e.g., transportation system with a low operative level). Specifically, the four roads connecting the marked cities on the left-hand side of Figure 5.5 (i.e., MSA255, SS148, SS156 and SS7) have operative levels of 0.5. The downgrade of the roadway system affects the mitigation efforts by civil protection personnel.

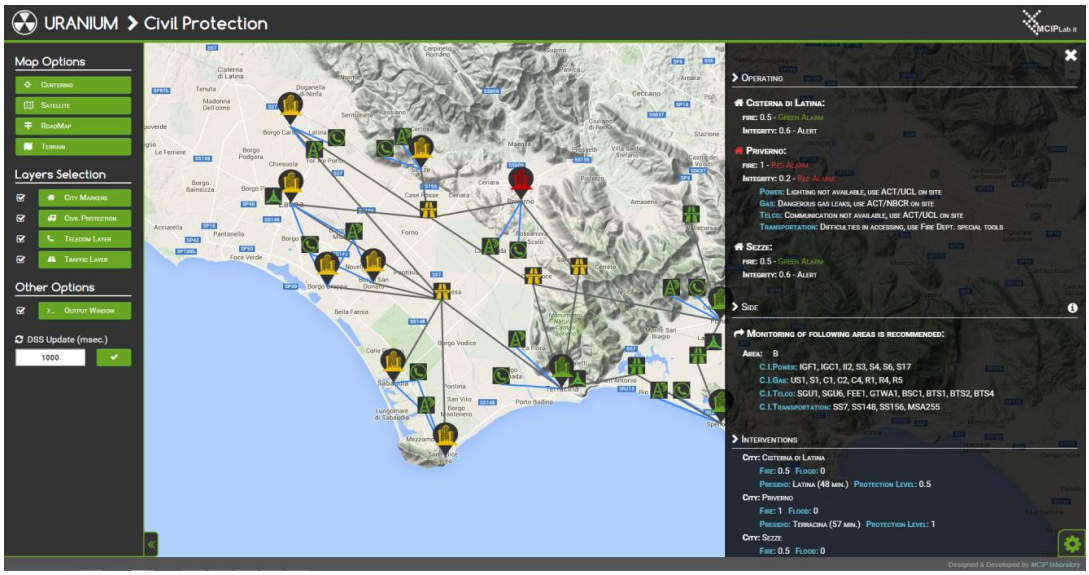


Figure 5.5 CISIApro URANIUM model.

Due to the modeled interdependencies, there is consequent risk propagation to the second primary substation (marked on the left-hand side of Figure 5.2a). This severely affects the power grid to the extent that it cannot meet the power demands of the cities connected to the second primary substation.

The ELECTRE II method used in this work defines a criteria/alternatives array whose elements express the enhancement of adverse event propagation caused by an emergency. Each criterion represents an objective function that is to be minimized. Different criteria such as adverse events, fault propagation levels and city populations are chosen in this research. The decision support system output uses the dominance principle to order the alternatives in descending order of priority. The alternatives correspond to the possible interventions that can be performed by civil protection units.

After the scenario and emergency alarm levels are defined for each area, the decision support system optimally allocates tasks to emergency operations centers based on

their distances and the recovery resources available in the districts. This method of resolution is chosen because it takes into account possible inaccuracies in the CISIApro model and strikes the right balance between data processing complexity and the time required to obtain solutions.

The customized decision support system panel presented in Figure 5.5 has three main components (shown on the right-hand side). The first is the "operating section" that summarizes the magnitudes of situations such as floods and fires and the operative levels of cities. The "side section" is where the decision support system lists the infrastructures that should be monitored. The third "interventions section" helps prioritize actions to be performed by each civil protection district to mitigate actual and forecasted critical issues. The estimated arrival times to perform interventions are also presented. A button on the panel is clicked to evaluate the mitigation actions; in each case, the positive propagation effects are presented based on a CISIApro simulation.

5.8 Conclusion

This work has demonstrated how decision support for critical infrastructure assets during emergencies can be enhanced using interdependency modelling. The approach is implemented in an innovative tool for studying the impact of catastrophes on interconnected critical infrastructures and optimally allocating resources and services immediately after infrastructure disruptions.

The CISIApro simulator is used to evaluate the consequences of adverse events in complex scenarios involving several interconnected critical infrastructures. The adverse events range from cyber attacks and mechanical faults to natural disasters. Using a decision support system in concert with CISIApro enables operators to make quick, informed decisions during adverse events.

We need to understand that a case study could involve many problems at the same time. Although, this work is mainly focused on a Disaster Recovery DSS, capable to optimizing resource for civil protection interventions, in the URANIUM project it was demonstrated how it is possible to have multiple DSSs (which use the same output provided by CISIApro simulator) are able to cooperate on the same scenario.

Summarizing, an important contribution of this work is the use of a single critical infrastructures model to support different downstream decision support systems. This approach has been experimentally validated on a realistic and quite complex case study of a smart area. The results show the effectiveness and the improvement of the proposed overall system.

Chapter 6

Dynamic Risk Analysis for Smart Grid Reconfiguration

Electrical grids are no more isolated infrastructures but they provide services towards other infrastructures and meanwhile water networks, telecommunications, gas pipelines and transport systems are mandatory in order to produce and deliver electricity. The reconfiguration algorithm determines the optimal tree configuration of the grid, after overloads or permanent faults. In literature, the reconfiguration algorithm takes into account feasibility, radiality, load balancing and energy losses.

The aim of this paper is to consider the effects of interconnected infrastructures on the reconfiguration algorithm. In order to realise this aim, we must collect information coming from heterogeneous infrastructures and normalize it. Thanks to CISIApro simulator is possible collect data on equipment operability by evaluating the cascading effects of faults, cyber attacks and natural disasters. The short-term forecast provided by CISIApro is the input of the decision support system for electrical reconfiguration purpose. This decision support system is made of two parts: an off-line tool able to generate a large number of possible configurations and a multi-criteria decision making (the on-line one) able to evaluate several criteria. The criteria are availability

of the telecommunication network for closing the needed switches, availability of the generators to supply the downstream loads, load balancing and, eventually, the blackouts or the unfulfilled loads, in terms of population and 'strategic' importance.

The algorithm has been tested on a scenario made of three interconnected infrastructures: distribution grid, gas pipeline, water distribution system and telecommunication network. Some results are explained for understanding how information fusion can improve decision support systems.

6.1 Introduction

Our lives are increasingly dependent on electricity and, therefore, attention to power grid resilience has increased in order to guarantee better and smarter decisions. The complexity of this problem is growing because power grids are no more a protected and isolated infrastructure, but they are interconnected with other critical infrastructures. Electricity supports the operations of other lifeline systems, such as communication networks, and key social systems, such as financial transactions. Other infrastructures provide services to power grids, such as SCADA (Supervisory Control and Data Acquisition) communication over a telecommunication network for remote control switches and fuel provided by gas pipelines for turbines.

Network reconfiguration is a very effective and efficient way to ensure load distribution of network's elements, to improve system reliability and voltage profile, and to reduce power losses. Taking into consideration a large number of switches in distribution network, whose on/off switching affects the network topology, reconfiguration problem can be defined as a complex combinatorial, non-differentiable, and constrained multi-objective optimization problem.

In literature, the problem considers only electrical aspects, such as voltage constraints or power losses. Electrical grid is also affected by external events, as failures

in interconnected infrastructures or natural disasters, that are hard to include in the classical formulation. Therefore, fusion of heterogeneous data is mandatory in order to assess the current situation and increase operators' awareness helping them with improved decision support systems.

6.2 Contributions

In this work, the authors describe how an interdependency model can be used in order to realize an intelligent distribution network reconfiguration algorithm. The interdependency model gathers unrelated data for several equipment providing normalized information to a downstream decision support system. In this paper the decision support system is for an electrical operator who wants to change the actual topology of the grid after a permanent failure in the grid itself, or after a natural disaster. The contribution of this paper is two-fold:

1. CISIApro is able to collect and fuse information for each modelled equipment. Each modelled entity within CISIApro produce an operative level, which is an aggregated risk metric.. Then, it also evaluates the quality of services towards other infrastructures and towards customers, as non-linear function of the single equipment involved in the service itself. CISIApro has been developed in order to understand how adverse events can be propagated and, therefore, it can be used to evaluate how equipment or services are affected by faults, disasters or cyber attacks.

2. It is applied a multi-criteria decision making algorithm (ELECTRE II) for evaluating the optimal reconfiguration considering the interdependencies with the other infrastructures. In particular, it is use an algorithm to develop a large number of possible configuration, checking the radiality of each configuration,

and considering the output of CISIApro in terms of available nodes and branches. Then, it is started ELECTRE II with several criteria, considering the output of CISIApro: availability of the telecommunication network for closing the needed switches, availability of the generators to supply the downstream loads, load balancing and, eventually, reducing the blackouts or the unsupplied loads, in terms of population and (strategic) importance. The results demonstrate how data fusion improves decision making.

6.3 Network Reconfiguration Problem

The reconfiguration of the distribution network is an important part of power system operations. Distribution networks are normally operated as radial tree; however, during operations, configuration is changed by means of sectionalizing switches. The operating configuration is a radial network, where each sink node is supplied from exactly one generator node. Therefore, the distribution network reconfiguration (DNRC) problem is to find a radial operating structure that minimizes the system power loss while satisfying operating constraints, [51] [52].

Two are the possible motivations behind the reconfiguration of the power grid: load balancing and service restoration, [53]. In event of the overloads, changing the topology can relieve this particular situation. Service restoration is the reaction process in event of a permanent fault made of three steps: isolating the faulted area; supplying the non-faulted area and minimizing the load shedding.

According to the graph theory, a distribution network can be represented with a graph of $\mathcal{G}(N, B)$ that contains a set of nodes N and a set of branches B. Every node represents either a source node (supply transformer) or a sink node (customer load point), while a branch represents a feeder section that can either be loaded (switch closed) or unloaded (switch open). The reconfiguration algorithm determines

an optimal tree of the given graph. The computational complexity of the optimal problem is very huge in large systems [54, 55] and, therefore, many heuristics have been developed in order to solve the reconfiguration problem [56].

The classical optimization problems consider the power losses of the electrical grid with two main constraints: feasibility and radiality. All nodes in the electrical grid must be connected by some branches to only one generator and the number of branches in the configuration must be smaller than the number of nodes by the number of generators. The simplest heuristic [51] is the branch exchange method, where the power losses are evaluated changing a pair of switches: close one and open another one at the same time. This method is easily understood but the solution is a local optima and depends on the initial network configuration.

In the last years, some researchers applied multi-criteria optimization algorithm to the reconfiguration problem. Usually, three objective functions are considered: minimization of power losses, minimization of deviation of node voltage and maximization of the branch capacity margin. Das in [57] evaluates these objectives through fuzzy sets considering their imprecise nature and solves it trough rule-based heuristic. An algorithm for reducing power losses and improving reliability on network reconfigurations is presented in [58] assessing the power losses on distribution and sub-transmission systems, promoting a global analysis on the impact of switching operations. In [59], the authors used a multi-criteria optimization algorithm for economic-related aspects: the cost of power losses and the cost of damages due to power supply interruption following some faults occurring into the distribution network.

One of the main challenge of the actual power grid is to face with the increasing amount of renewable resources. In [60], the authors propose a multi-period optimal power flow approach for assessing the improvement of distributed generation hosting capacity of distribution systems by applying static reconfiguration or dynamic reconfig-

uration, together with active network management schemes. In [61], the reconfiguration problem is analysed together with the optimal placement of renewable resources by means of a meta heuristic Harmony Search Algorithm.

The increasing use of remote controlled equipment in power systems leads the development of more efficient techniques for automatic reconfiguration of network, being particularly important in Smart Grid applications. In [62] presents a methodology and system for automatic reconfiguration of distribution network in real time. The optimization of the network performance is based on a heuristic method and multi-criterial analysis, based on the Analytic Hierarchic Process (AHP) method to define weights for the optimization criteria and to determine the best sequence of switching for the network.

In this paper, we consider an active network management for the electrical distribution grid, where each switch can be remotely telecontrolled from the SCADA control centre through a telecommunication network. In order to take into account the interdependencies among the electrical grid and other infrastructures (such as, telecommunication networks, gas pipelines and water distribution system), a framework able to collect and normalize all the information coming from heterogeneous fields is mandatory. CISIApro is an agent-based simulator for analysing the consequences of malfunctioning within interdependent critical infrastructures. In order to improve the situation awareness of distribution system operators, a smart decision support system is mandatory realised by means of a multi-criteria algorithm. We choose an improved ELECTRE II method [49]. ELECTRE II meets the required performance by introducing innovative aspects, such as the threshold values to model the uncertainty of available data. The choice fell upon these methods of resolution because it takes into account possible inaccuracies in CISIApro model and achieve the right balance between complexity of data to be processed and the time required to get the solution.

6.4 Proposed Architecture

CISIApro platform is based on CISIApro engine, to calculate the cascading effects through the interdependency model, and on CISIApro GIS (Geographical Information Security) to geo-reference the critical infrastructures' elements of the case study.

CISIApro is a software platform based on a database-centric architecture in which the database plays a crucial role. This means a centralized asynchronous design that allows a good modularity and scalability where each element of the informatics infrastructure interfaces, independently, with the centralized database (DB) in order to get the last actualized data from the field, as in Figure 6.1.

From this point of view, CISIApro engine does not only analyse actual situation and calculate the risk projected in the possible next future but, first of all, it plays the important role of Hybrid Risk Evaluation Tool. Hybrid because it is able to get information of different natures (sensor and data acquisition and complex event processing systems) and translating them in operational levels of resources, faults or services for the entities introduced in the critical infrastructure model.

For example, we can image an information system where we have not only data acquisition from common sensors but also data regarding malfunctions reported by users. This means different kinds of data to assess the risk of actual ongoing situation.

As we can see, in Figure 6.1, we have a schematic representation of CISIApro platform architecture where we appreciate the modular design and the DSS (Decision Support System) data processing structure.

At the same time, with this architecture, we are able through CISIApro modelling software to dynamically change the interdependencies model and plug-in other modules (like Decision Support System modules) in order to have a real-time scalable and flexible system which can be changed at any time.

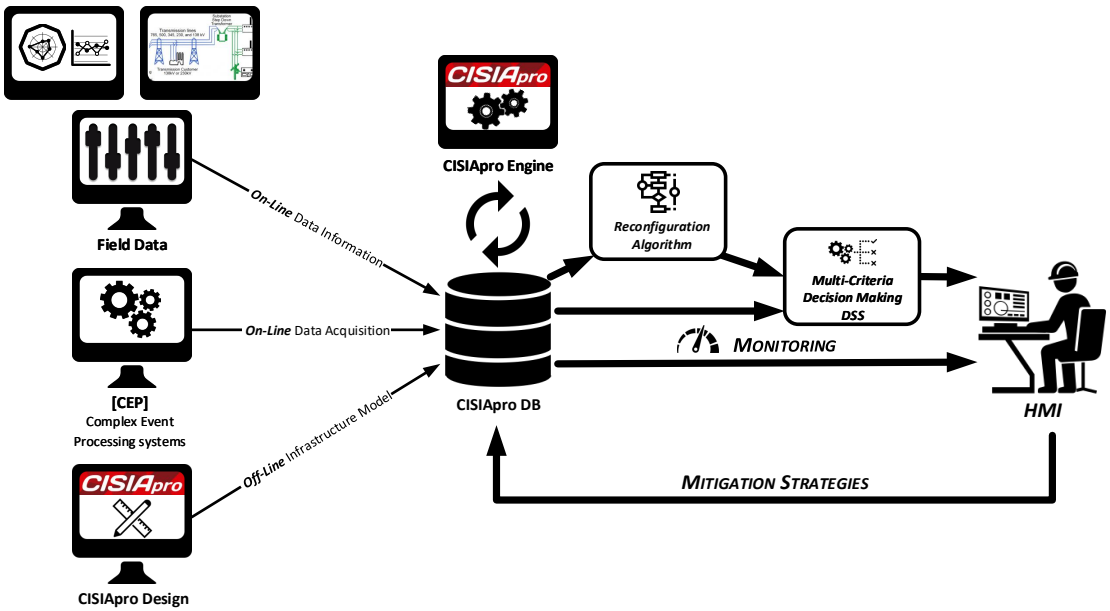


Figure 6.1 Proposed architecture.

The data stored in the database comes from the field and from, eventually, a Complex Event Processing (CEP) algorithm to track and analyse streams of information about events that are happening, in Figure 6.1. Once the state variables are modified, CISIApro Engine automatically detects the change of system state and runs a simulation instance to calculate the cascading effect. Afterwards CISIApro stores produced data associating a unique run id, see Figure 3.4. Then, the network reconfiguration algorithm is executed and the possible reconfiguration are sorted thanks to the Multi-Criteria Decision Making and visualized to the electrical operator. Eventually, the reconfiguration can be applied into the reference scenario for evaluating the consequences in the system.

In this way, any downstream module can get data regarding the latest critical situation in the modelled scenario. On the same scenario, the electrical distribution network reconfiguration algorithm is capable to recognize the power grid configuration in order to produce and communicate all possible network reconfigurations to the DSS

module. Only subsequently, the DSS will be able to exploit all possible reconfigurations through the assignment of the risk levels calculated in real-time by CISIApro.

The data flow ends with the output in CISIApro GIS where all critical infrastructures are displayed through an intuitive interface along with the ranking of possible configurations and with some suggestions for the operator for increasing the operative levels of involved entities. It is also made available a button to simulate the effects of suggested reconfiguration by decision support system.

6.5 Problem Formulation

In this section, the electrical distribution network reconfiguration problem is explained, describing involved algorithms in the framework.

6.5.1 Electrical Distribution Network Reconfiguration Algorithm

The reconfiguration algorithm is an off-line tool able to generate all the possible configurations for the electrical distribution network in the considered scenario, see Section 6.6. This algorithm takes as input the electrical topology, expressed as a graph $\mathcal{G} = (N, B)$ containing a set of nodes N and a set of branches B. The nodes contain a subset of generators that are NG. The algorithm generates all configurations respecting two constraints:

- Feasibility: all nodes are connected to a generator (i.e., no isolated node are possible);
- Radiality: only one generator can feed a load.

The resulting configurations are a forest, i.e., a set of trees starting from a generator. In other words, we consider only configurations with not more than $N - NG$ branches.

In event of a load failure, the feasible configurations contains exactly $N - NG - NF$, where NF are the number of faults at load level.

6.5.2 Multi-Criteria Decision Making: ELECTRE II

Single criteria optimization was the approach adopted for managerial decision problems for years. It is a mathematical method used to search the optimal solution (maximum or minimum) of a decision problem when the pursued aim is unique and it is subject to multiple constraints. If we want solve complex problems, with more objectives and constraints, the single criteria optimization approach is too simple and the model can not match with problem to be solved.

In this context, multi-criteria analysis methods allow us to compare and sort the alternatives according to the problem's objectives, that are often at odds with each other. These methods, in contrast with the classical techniques of operational research, don't provide solutions objectively good, but they provide a support to the decision-maker to achieve an acceptable compromise between the various objectives pursued.

The ELECTRE methods family stems from the idea that the rigorous mathematical axioms cannot describe a complex reality such as the decision-making process, which is characterized by many contradictions. Their purpose is to develop a method that faithfully adheres to reality. They follow the decision irrationality and they reject the completeness theorem, expressed as "*the decision maker, faced with two alternatives, must be always able to express his preference or indifference*". The ELECTRE II ranks the alternatives from the best to the worst, using the outranking relation whose meaning is "at least as good as", see also [49].

We consider a situation with one decision maker, with m alternatives and n criteria or attributes, where the alternatives are explicitly listed using the notation $A_1, A_2, \ldots, A_m$.

The ELECTRE II method is defined by a $m \times n$ matrix, called decision matrix and denoted with C, where each element c_{ij} evaluates the alternatives i according the the j criterion. In general, not all the attributes are numerical, but it is mandatory to map the qualitative attribute into an arbitrary numeric value maintaining the same ranking of the alternatives.

Two kind of analyses allow the verification of outranking relationships between two alternatives:

1. Concordance analysis consists in an analysis of those factors and criteria which do not oppose to the fact that one alternative might be preferred to another;

2. Discordance analysis defines the regret to choose an alternative instead of another

The ELECTRE II method creates an outranking relationship among the alternatives, using also a weight w_j for each criterion j, representing its relative importance respect to the other criteria. The key concept is that A_h *is preferable to* A_k if:

- Great satisfaction is achieved preferring A_h to A_k;

- No great dissatisfaction is obtained in preferring A_h to A_k

Let us consider the definition of preference P_j.

Definition 6.1. *Given two different alternatives, A_h and A_k, A_h is preferable to A_k according to the j criterion, denoted as $A_h P_j A_k$, if $c_{hj} \geq c_{kj}$.*

Definition 6.2. *Given two different alternatives A_h and A_k, A_h dominates A_k, in symbols $A_h \geq A_k$, if $c_{hj} \geq ckj$ for each criterion $j = 1, \ldots, n$.*

ELECTRE II method is usually divided into three stages.

Stage I In this stage, the method evaluates the concordance matrix C_{hk} and the discordance matrix D_{hk}, for every couple of alternatives $(A_h, A_k), h \neq k$.

The concordance matrix takes into account the weight of the criteria according to which h is preferable to k:

$$c_{hk} = \frac{\sum_{j:A_h P_j A_k} w_j}{\sum_j w_j} \tag{6.1}$$

The discordance matrix takes into account the criterion most opposing to the preference of h to k:

$$d_{hk} = \max_{j:A_k P_j A_h} \left\{ \frac{c_{kj} - c_{hj}}{diffMax_j} \right\} \tag{6.2}$$

where $diffMax_j = \max_j\{c_{hj} - c_{kj}\}, h = 1, \ldots, n, k = 1, \ldots, n$.

Stage II Let us introduce some veto thresholds, strong f and weak d, to assess the alternatives outranking. Two concordance thresholds S_C^d and S_C^f are introduced such that $0 < S_C^d < S_C^f < 1$. If $S_c \to 1$ then only one concordance value exists and no conflict is generated where choose one alternative with respect to another one. Two discordance thresholds S_D^d and S_D^f are introduced such that $0 < S_D^f < S_D^d < 1$. If $S_D \to 0$, then it means that we can choose with no regret one alternative with respect to another one.

Therefore, two outranking relationships can be defined: weak and strong outranking.

Let us define *weak outranking* $A_h S_D A_k$ between two alternatives A_h and A_k if and only if $c_{hk} \geq S_C^d$ and $d_{h,k} \leq S_D^d$.

Let us define *strong outranking* $A_h S_F A_k$ between two alternatives A_h and A_k if and only if $c_{hk} \geq S_C^f$ and $d_{h,k} \leq S_D^f$.

We obtain two graphs, one weak and one strong, enhancing the level of available information and making the choices more accurate. The strong graph is more rigid and strict, with few outranking relations and many incomparability relations.The weak

graft is less restrictive and richer in outranking and presents fewer incomparability relations.

Stage III Using two different order algorithms, one ascending and one descending, it is possible to obtain the final alternatives' classification. In this stage in particular, the algorithm elaborated during the research and tested several times during the simulation stage includes the following sequential operations:

1. Calculate the aggregated weak dominance matrix E^d as node/node incidence matrix of the weak outranking graph

2. Calculate the aggregate strong dominance matrix E^f as node/node incidence matrix of the strong outranking graph

3. Calculate the aggregate dominance matrix $E = \{e_{hk}\} = E^d + 2E^f$

4. Calculate the alternatives' score in accordance with two orders: the sum in each column e_h^c of the matrix E is calculated for each alternatives h, and the sum in each row e_h^r of the matrix E is evaluated.

5. Calculate the alternatives' classification: for each alternative h we obtain $e_h = e_h^c - e_h^r$ and then the alternatives are ordered according to e_h values.

The final classification of the alternatives is given by the arithmetical sum of the scores obtained from the described orders. The alternatives' classification is obtained using a matrix approach instead of a graphic one, as proposed in the original version of the ELECTRE II algorithm.

In the reconfiguration problem, the alternatives are the feasible reconfigurations, as a list of closed/opened switches. The criteria represent the alternatives sort algorithm, according to electrical operator preferences. We consider eight criteria:

1. **Active healthy switches**: we consider the average value of the closed switches' operative level, where a "healthy" switch means an electrical breaker that can be remotely telecontrolled;

2. **Active healthy generators**: we consider the average value of active generators' operative level, where a "healthy" generator means a generator with low risk of producing power;

3. **Number of active generators**: we prefer configurations with more active generators, in this way the grid is balanced among the generators;

4. **Healthy changing switches**: we consider the average value of the changing switches' operative level, where a "healthy" switch means an electrical breaker that can be remotely telecontrolled;

5. **Hops number**: each hop represents a switch status change, starting from the actual configuration to obtain the particular configuration. We prefer configuration with low hops, according to a low energy profile;

6. **Configuration strategic value**, implemented as the average value of the active switches' strategic value. Each switch has a value based on its strategic importance;

7. **Black-out dimension**: we consider the amount of loads not feed by the grid;

8. **Population involved**, as the population negatively affected by the black-out obtained by particular configuration.

6.6 Case Study

This paragraph describes the case study used to validate the overall system. The aim is to understand how data fusion can improve the distribution network reconfiguration in an interdependent scenario. We consider three main infrastructures: a distribution electrical grid and a gas pipeline which guarantees the fuel for one turbine generator of the electrical grid; both the electrical and the gas grids are controlled by two distinct SCADA control centres by means of an Ethernet-based telecommunication network.

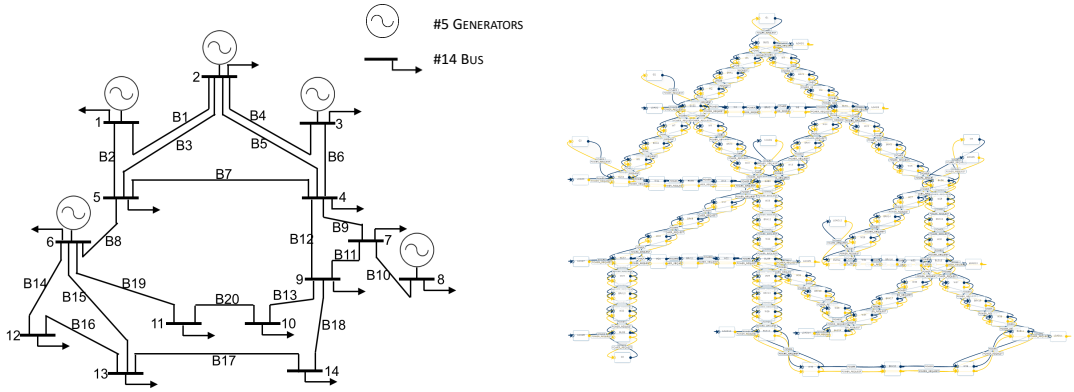
The power grid has a mesh topology and it has five generators, where one of them is a gas turbine unit and the others are solar and wind farm and two substations from the electrical transmission grid.

The distribution gas pipelines have a radial topology from the regulator connected to the gas transmission network. The model considers a set of pumping stations maintaining constant the gas pressure by means of compressors. If a leakage happens or if a compressor is out of order, the storage supplies the gas pipelines to fed customers. The natural gas is also used as fuel for an electric generator connected to circuit breakers. Electricity is needed for pumping stations and regulators within the gas pipelines.

Both those two infrastructures have a SCADA control centre, able to collect data from sensors and change pre-defined threshold for generators. Those SCADA control centres make use of an Ethernet-based telecommunication network.

The telecommunication network has a mesh structure and is made of optical fibre. We model it for land-line and mobile services, for understanding how coordinate crises. Telecommunication network is actually used among electric and gas SCADA control centre and field sensors. Telecommunication routers and switches need electricity to proper work.

The electrical grid is the IEEE 14 busbar test system [63], in Figure 6.2a, and its implementation within CISIApro is depicted in Figure 6.2b. The electrical grid is an



(a) IEEE 14 busbar test system scheme (b) CISIApro 14 busbar Implementation

Figure 6.2 The electrical distribution network.

active network where each switch can be opened or closed from the control centre, changing the actual topology in event of overloads or permanent fault. Each branch has a sectional switch that can be telecontrolled. In Figure 6.2a, the busbars are numbered from 1 to 14, and the switches on each branch are enumerated with the symbols $Bi, i = 1, \ldots, 20$. For example, $B1$ is the switches number 1 between busbar 1 and 2, and so on.

In this scenario, we consider the following situations as meaningful:

- Fault on a compressor within the gas distribution network. The compressor in the pumping station maintains constant the gas pressure and, in event of failure, the loads and also the gas turbine of the power grid (specifically, the generator connected to busbar 2, see Figure 6.2a) can be without the right amount of fuel and the risk of the generator is increased due to possible fuel unavailability;

- Cyber attack on the telecommunication network, such as a Denial of Service (DoS), see also Chapter 4. In this case, the partial unavailability of telecommunication network causes problems on the controllability of the electrical switches.

- A fire occurring near load 13, causing a permanent fault at the bus level. Firstly, the bus is isolated, opening automatically the switches (in particular switch 16 and 17 in Figure 6.2), and then another configuration can be chosen in order to increase the reliability of the network

The initial configuration of the electrical grid is the following one:

– switches $\{B2, B5, B9, B12, B13, B14, B15, B18, B19\}$ are CLOSED;

– switches $\{B1, B3, B4, B6, B7, B8, B10, B11, B16, B17, B20\}$ are OPEND.

We observe that two generators just feed the loads connected the same busbar: considering the initial configuration, generators on busbar 3 and on busbar 8 are islands (or eventually micro-grids) feeding the loads connected to the respectively busbars. In Figure 6.2a, the loads are represented by arrows coming out from the busbars.

6.7 Results

In this paragraph, we comments the results obtained from the framework and how data integration improves decisions. As already described in the previous paragraph, we consider three different situations. Nevertheless, real situations could also include several adverse events in a subsequent order.

ELECTRE II is an almost automated approach that involves minimal intervention by the decision maker, which, apart from having a crucial role in the final choice, is also the main actor in the definition of an important magnitude value, represented by the criteria weights. They must be attributed to each basic criterion according to operator' judgements and opinions. The variation of these magnitudes can lead to different results, maintaining unaltered all the other conditions. Obviously there is a default configuration where we consider the weights perfectly balanced but a particular

configuration of the criteria weights can be set, depending on the scenario and the events that the operator is to manage. A weight equals to zero does not mean that the criterion is not considered but its valued less than the others.

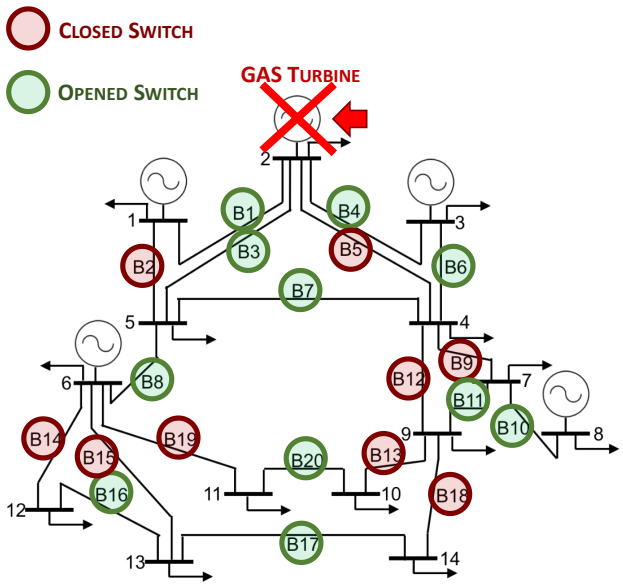


Figure 6.3 Experimented situation 1.

Situation 1. Fault within the gas distribution network - Figure 6.3 In this situation, CISIApro evaluates the cascading effect of a fault at the compressor within the pumping station in a gas pipeline. The generator number 2 (connected to busbar 2 in Figure 6.2) is a gas turbine fed with natural gas provided by the pipelines. In CISIApro the operative level of the generator is equals to 0, corresponding to a high risk.

After CISIApro execution, a first step in the decision making process is the definition of the list of all the feasible configurations. After this step, the ELECTRE II algorithm is executed with weight w_j for each criterion. The weights in this situation are described

following the list provided in the final part of Section 6.5.2:

$$W = \{w_j\} = \{0, 0, 1, 0, 0, 0, 0, 0\} \tag{6.3}$$

where the electrical operator prefers a configuration with a high number of generators, i.e., the third criterion.

In Table 6.1, the five better configurations are listed in descending order from the preferred one, with the evaluation of each criterion. We include just six of the eight criteria, because the last two, related to the blackouts, do not discriminate the alternatives. The symbols in Table 6.1 $\{C1, C2, C3, C4, C5, C6\}$ denote the criteria in the same order as in Section 6.5.2, for example $C1$ is the mean vale of the operative level of the closed switches, and so on.

Table 6.1 Sorted results in descending order for situation 1, when the gas turbine is at high risk: the first configuration is the best one. The configuration is expressed as a list of closed switches.

Configuration	C1	C2	C3	C4	C5	C6
$\{2, 6, 10, 13, 15, 16, 17, 18, 20\}$	0.98	1	4	0.97	0.33	1
$\{2, 6, 10, 12, 13, 15, 16, 18, 20\}$	0.97	1	4	0.98	0.47	1
$\{2, 6, 10, 12, 13, 14, 15, 18, 19\}$	0.97	1	4	0.95	0.73	1
$\{6, 8, 10, 11, 15, 16, 17, 19, 20\}$	0.99	1	3	0.96	0.07	1
$\{2, 5, 10, 13, 14, 15, 17, 18, 20\}$	0.97	0.75	4	0.97	0.6	1

Situation 2. Cyber attack on the telecommunication network - Figure 6.4
In this case, CISIApro evaluates the consequences of a Denial of Service within the telecommunication and its effects on the physical system, see also Chapter 4 for more detailed information. The consequences of this cyber attack is a high risk for a set of switches, i.e., switches number 8, 10, 16 and 19 in Figure 6.2 have operative level equals to 0. The criteria weights $\{1, 0, 1, 0, 0, 0, 0, 0\}$ prefer configurations with a greater number generators and "healthy" switches involved in the reconfiguration. In normal

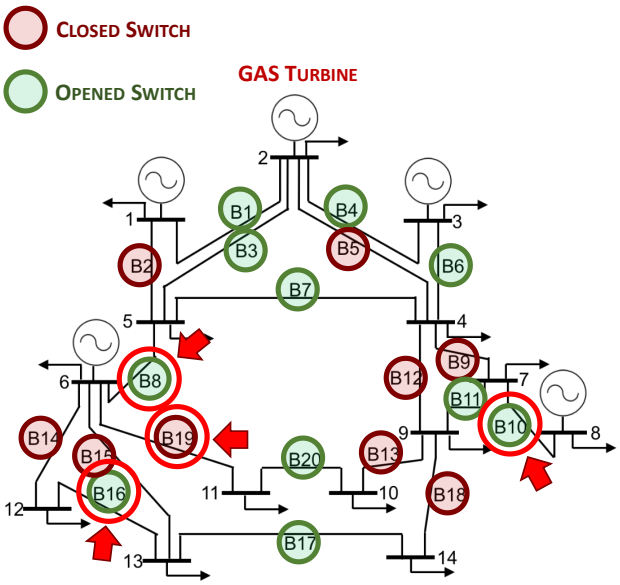


Figure 6.4 Experimented situation 2.

situation for the power grid, the loss of controllability can be a minor problem, but in event of overloads the operator may change the topology and could not do it due to problems on the telecommunication network. We also change the strategic value of each switch:

- Switch 01 = 0.05
- Switch 02 = 0.10
- Switch 03 = 0.15
- Switch 04 = 0.20
- Switch 05 = 0.25
- Switch 06 = 0.30
- Switch 07 = 0.35
- Switch 08 = 0.40
- Switch 09 = 0.45
- Switch 10 = 0.50
- Switch 11 = 0.55
- Switch 12 = 0.60
- Switch 13 = 0.65
- Switch 14 = 0.70
- Switch 15 = 0.75
- Switch 16 = 0.80
- Switch 17 = 0.85
- Switch 18 = 0.90
- Switch 19 = 0.95
- Switch 20 = 1.00

where 1.00 means very important switch.

The results are summarized in Table 6.2 in descending order. Among the feasible configurations, there are also three configuration where the switch 10 is telecontrolled from opened to closed status, in any case. The results of the multi-criteria decision making are not easily to understand due to the large amount of criteria, weights, thresholds and parameters.

Table 6.2 Sorted results in descending order for situation 2, caused by a Denial of Service. The configuration is expressed as a list of closed switches.

Configuration	C1	C2	C3	C4	C5	C6
$\{2, 5, 11, 13, 14, 15, 17, 18, 20\}$	1	1	3	0.83	0.6	0.64
$\{2, 6, 9, 13, 14, 15, 17, 18, 20\}$	1	1	3	0.83	0.6	0.63
$\{2, 6, 10, 13, 14, 15, 17, 18, 20\}$	0.89	1	4	0.75	0.47	0.64
$\{6, 7, 10, 13, 14, 15, 17, 18, 20\}$	0.89	1	3	0.8	0.33	0.67
$\{2, 6, 10, 11, 13, 14, 17, 18, 20\}$	0.89	1	4	0.8	0.33	0.62

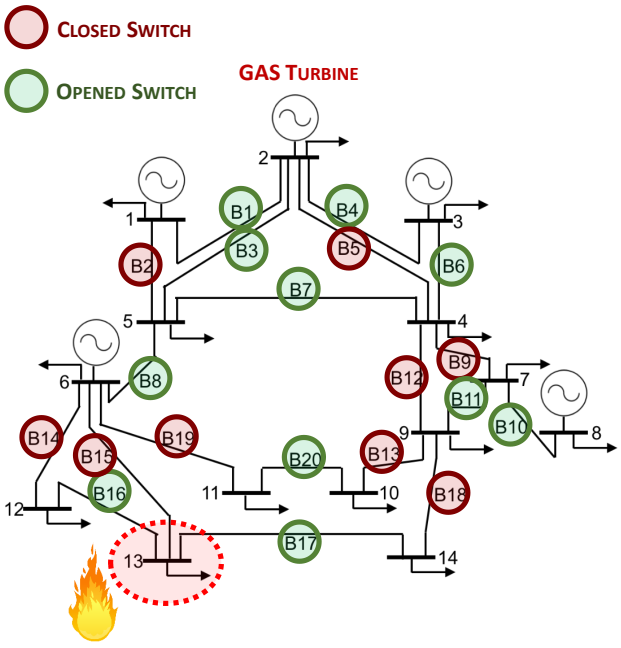


Figure 6.5 Experimented situation 3.

Situation 3. A fire occurring at load 13 - Figure 6.5 CISIApro evaluates the consequences based on a geographic propagation of the fire event: near the fire, all the equipment are at danger. The electric grid must isolate the fault opening the sectional switches around the busbar 13.

The feasible reconfigurations obtaining closing one switch less than before are more than 6.000. In the previous situations, the number of feasible configurations was around 2500.

The criteria weights prefer a configuration with a major number of generators, as in situation 1.

The results for the five better configurations are presented in Table 6.3, without considering the number and the population involved in blackout, that are at busbar 13.

Table 6.3 Sorted results in descending order for situation 3, caused by a fire around busbar 13. The configuration is expressed as a list of closed switches.

Configuration	C1	C2	C3	C4	C5	C6
$\{2, 5, 6, 10, 13, 14, 18, 19\}$	1	1	5	1	0.67	1
$\{2, 3, 6, 10, 13, 14, 18, 19\}$	1	1	5	1	0.53	1
$\{2, 3, 5, 6, 9, 10, 14, 18\}$	1	1	5	1	0.53	1
$\{2, 3, 6, 7, 10, 13, 14, 18\}$	1	1	5	1	0.4	1
$\{2, 3, 5, 6, 7, 10, 14, 18\}$	1	1	5	1	0.4	1

6.8 Conclusion

The distribution reconfiguration problem is an example of decisions that an electric operator must make every day during his work. This decision is usually made considering only the information related to the electrical grid itself. Nowadays, the electrical grid has a web of interconnection with other critical infrastructures, such as telecommunications and gas pipelines. Those interconnections make even harder every decision. Fusing information improves the operator awareness.

This paper demonstrates how information integration, realised using CISIApro, enables multi criteria decision making. CISIApro is an agent-based simulator for forecasting the consequences of adverse events in a scenario made of interconnected infrastructures. In this way, CISIApro can be also considered as an integration platform of heterogeneous signals coming from the field.

CISIApro results are used as input of a decision support system. ELECTRE II is a method of the multi-criteria decision making, which simulated the operator process in decision but in automatic way. ELECTRE II is devoted to rank the alternatives, i.e., the feasible configuration, following several criteria. Those criteria can also be very different between each other.

In this paper, the criteria represent how the other infrastructures affect the reconfiguration problem, a well known problem. The results show how the proposed framework is flexible and can handle also large amount of alternatives, but with good performances in terms of computational time. The case study presented is an example of how this framework can be exploited.

This framework can suffer of out-of-memory due to the number of feasible configurations. This problem can be solved reducing the number of configurations, considering explicitly one or more criteria, within the selection algorithm, see Section 6.5.1. Another possibility is to reduce the matrices dimensions of ELECTRE II (that are usually causing the out-of-memory problem) in the following way: dividing the problem into sub-problems of 1000 alternatives, choosing the better configuration respect to the others, and finally executing an ELECTRE II method among the optimal configurations of each sub-problem. With this approach, we can eventually improve the computational time using parallel programming, without precision loss.

Ongoing work is related to the inclusion of electrical criteria within ELECTRE II, such as the power losses, and eventually the comparison between the standard formulation and the results of this paper.

Chapter 7

Dynamic Risk Analysis for Organization Business Continuity

When we speak about Critical Infrastructure for Business Companies one of the main topic, is: How can we integrate dynamic Risk Assessment respect to Business Continuity needs? How it can be linked with the different aspects of reality like cyber, physical, geographical, logical, economical and so on? From these point of view, is it possible to improve the resilience in the enterprise context? In this chapter, we propose a specific framework able to solve these problems, tying concepts belong to different realms: Critical Infrastructure Protection and Business Continuity. Our solution is able to maintain high performance levels, in unfavourable situations, reallocating the available human resources. The proposed model, through interdependencies, takes into account different aspects and resources: as case study, we chose a typical medium-size organization with its main assets (Buildings Availability, Human Resources, corporate ladder and primary services like power supply, TELCO and water supply). Our aim is to ensure high-quality performances in work contexts. To demonstrate the validity of these concepts an agent-based simulation was created. Furthermore, we consider an integrated architecture with a supervisory and control systems able to collect data

from building sensors and building access control system. These informations are used for both initial condition in the simulation and as updating for system state variables. Thanks to the cascading effect and modelled interdependencies the simulation produces a dynamic risk evaluation about a 'possible' next future. Finally, a Decision Support System able to reallocate available human resources is proposed. The DSS takes into account employees skills and the business units strategic values (also known as strategic business impact).

7.1 Introduction

It is no secret that, in modern society, technological development must be powered, encouraged and supported by an economic strength closely linked to business aspect. And this applies to all the sectors that providing primary services to support human activities. These infrastructures are frequently affected by catastrophic events which involve discontinuity or complete interruption to provided services.

They cannot be forgotten socio-economic consequences due to the recent terrorist attacks or natural disasters like Hurricane Katrina [October 2012] which represents an interesting case study to investigate from the perspective of interdependencies between specific critical infrastructures (CIs) sectors [64]. All these events form part of our cultural heritage must necessarily be converted into valuable lesson for the future.

It is generally accepted that the combination of one or more active failures and latent conditions are followed by indirect damages due to business interruption. These kinds of indirect damages resulted primarily from interconnected risks within infrastructures. For these reasons, to have a coherent and compressive critical infrastructures model, agent-based (ABM), is mandatory. It must be borne in mind that, like power distribution system is a key sector for water distribution, TELCO, Gas & Oil distribution

and so on, intellectual activity supplied by people is the lifeblood that feeds every productive process at the basis of our society.

Nobody can predict with any certainty what the future holds but emergency preparedness and response and contingency planning, in critical situation it is a duty towards our modern society and a gateway to improve CIs resilience. Enterprises are constantly exposed to risks of different nature that came from: natural disasters, power outage, transport network, international agreements, economic and financial crisis and so forth. A first risks distinction, with respect to existing interdependencies, should be made by identifying *sources of internal risk* (from the Business Ecosystem) and *sources of external risk* (from the outer world) Figure 7.1.

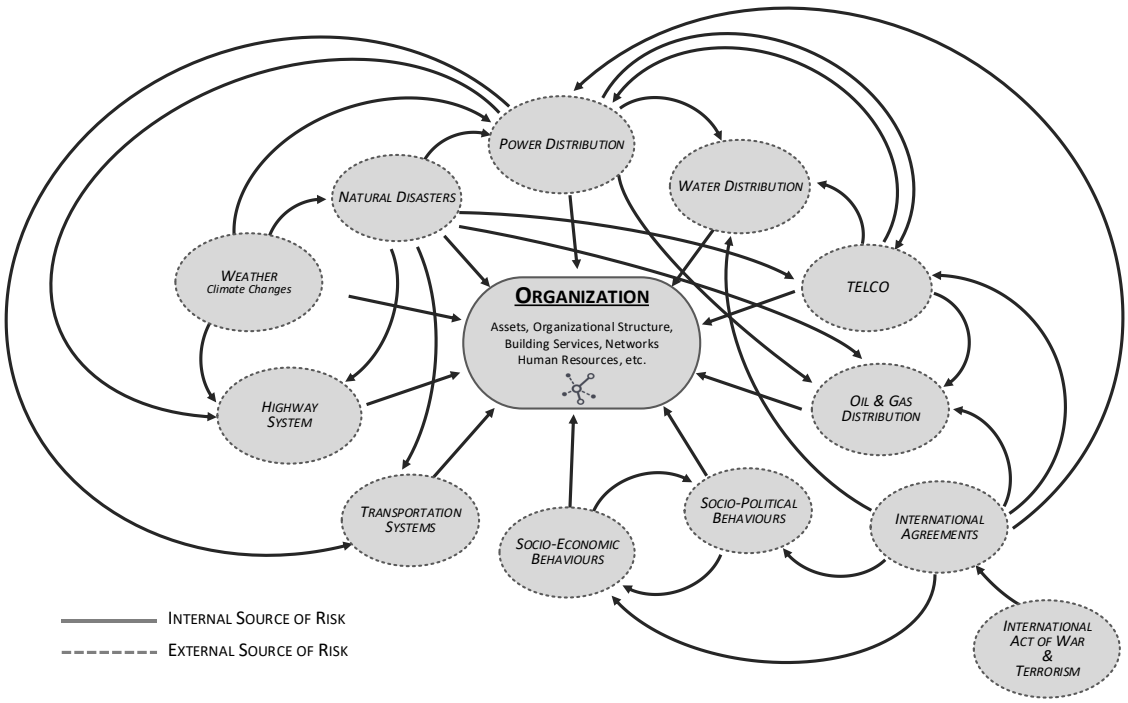


Figure 7.1 Internal and External Risk Interdependencies.

'Business Continuity Management' (BCM) has been defined as:

> ***BCM*** *– holistic process that identifies potential threads to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.*
>
> [ISO 22301] [65]

It is clear that when the CI model include outside interactions not all informations are available due to the information sharing problem. In this work we are focused on internal organization ecosystem dynamics using an *Asset-Based approach* business oriented, however, we can extend such approach to any external source of risk when we need. The Asset-based approaches take on the general aim to identify and mobilize assets that can be used together and in various combinations [66]. At the heart of all these mechanisms, there are 'people' and through their skills and workforce, they makes enterprises more robust and resilient with respect to unexpected events. An appropriately Human Resource allocation ensures a proper execution of the considered business process, in order to have an effective BCM.

The terrorist attacks of 11 September 2001 have casting shadow over the world leading debates on significant provision to change BCM practices taking into account enterprise/organization resilience along with resilience by employees to improve a smart recovery in large-scale scenarios [67].

According to CA Technologies research report (*The avoidable cost of downtime*), it is estimated that the revenues are reduced by one third when corporate critical systems have an interruption [68]. Other Chartered Management Institute study underlines that during the last year, about 40% of the organization has suffered losses due to

IT issues. It can be said that perturbations like extreme weather conditions, loss of skilled personnel, loss of telecommunications and network interruptions could be affect BC [69].

Risk Management, Security management, and Business Continuity Management are designed to protect information and guarantee continued operation within an organization. However, boundaries are *'fuzzy'* and it is hard to isolate all disciplines which dealing with recovery programs following an accident that threatens an enterprise from internal or external sources of risk. It is important to consider the fact that most disciplines are closely linked through crossover areas [70].

It becomes even more difficult when combination of this disciplines are strictly associated to operational management process because stakeholders, from very different backgrounds (e.g.: decision makers, business owner, re-engineering and business continuity experts), use different techniques and tools to achieve their objectives. Accordingly, there is not a common language or a consolidated and integrated approach, on the one hand, able to sustain safety, security and continuity and, on the other, to support economic perspective. As an example of how issues arising from different perspective could be the practice to use redundant resources. In certain cases of BC, redundant resources, are highly recommended but also produce vast increases from the economic point of view. Limiting this aspect is already one of the most important challenges into *Business Process Management*.

Currently, traditional Business Process Management and Management Support Tools do not takes into account how important is to share skilled human resources between internal production processes. This sharing should be enhanced especially during critical situations in order to reduce losses due to business discontinuity. Business Continuity (BC) stems from the need to maintain high quality of service and productivity upon the occurrence of:

- IT-related issues;
- lack of resources to set up business productivity process;
- destructive events like natural disasters or economic crisis.

Ultimately, the main BC objectives are:

- increase ***resilience***;
- speed up ***recovery*** procedures;
- reduce ***exposure*** risk due to security systems;
- decrease ***impact*** of catastrophic events;
- respond quickly to any kind of ***thread***;
- turn critical situations into new ***opportunities***.

Business Continuity is directly linked to Risk Assessment and must be successfully integrated with existing business processes. Adoption of such strategies have an intrinsic value in themselves and create new opportunities, while, mismanagement should be cause short and long-term losses also in term of *company credibility* and *loss brand value*.

Despite these issues are familiar, only two-third of big organisations has developed efficient BC strategies [71]. Probably, such behaviour, is due to short-sightedness of top management, their inability to allocate resources to BC but mostly to the lack of clearly and consolidated framework simply to introduce into pre-existing enterprise mechanisms. To manage and restore normal activities, in situation of high risk and inefficiency, it is necessary to refer to system architectures that are able to guarantee real-time reaction with low latency in response time. Anyway, it is important maintain high standards of safety and security with welfare in social and work settings.

7.2 Contributions

In this work a new framework for BC is proposed. Such approach take into account some concepts, applied to the critical infrastructure protection, based on Risk Assessment and Risk Prediction. The authors provide the overall process using a 'centric' hybrid validation system Chapter 4 capable to connecting to real-time environment (or pseudo real-time) like data acquisition systems (e.g. SCADA system or IoT ecosystem), access control systems, complex event processing systems and external data sources.

In particular, starting with modelling a buildings of an enterprise and introducing the Organisational Management Structure (defined by an Organisation Chart), performance metrics for BC are produced. These kind of metrics are results of interdependencies among different aspects like: strategic evaluation of enterprise assets, level of 'Information Sharing' in connection with departments and the 'Quality of Service' (QoS) offered by the corporate building.

Thanks to these evaluations four sequential ILP (Integer Linear Programming) problems are formulated in order to maximize the overall business performance reallocating 'human' resources. This approach is innovative in BC context because is hard to find procedures and algorithms able to take into account complex interactions that exists among the enterprise organization, human behaviours, skills & capabilities, personnel crises such as large scale staff illness or death, loss of utilities (gas, power supply, water, telecommunication and so on) and it raises the question of how 'Indoor Environmental Quality' (IEQ) affects occupant 'Quality of Work' (QoW) [72]. The validation of this process was realized with an emulated IoT environment using a gateway-based architecture.

7.3 Business Continuity Management & Risk Assessment

Business Continuity Management is a very wide sector and, reaching a common goal among different optimization strategies (i.e. optimal assets reallocation in critical situations), is a quite challenging task. Moreover, introducing Critical Infrastructure Protection concepts and techniques in the design of BCMs tools, lead to complex problems in the identification of a general framework. Hence, designing efficient BCM procedures is mandatory to decide which aims cover and pursue. In the following, possible scenarios where CI protection and BCM are tied together, are introduced:

- **Lack of Infrastructure**
  - Power outage, Gas outage, Water outage, IT network outage, Technology connection outage, Loss of data, System application outage, Telecoms outage, Flood, Fire, Earthquake;
- **Lack of Access**
  - Power failure, Road closure, Fire, Flood, Bomb, Water outage, Gas leak, Bomb alert, Structural damage, Area evacuation;
- **Lack of People**;
  - Contagious illness, Strike, Transport outage, Building closure.

In [73], the authors propose a framework for BCM of CI integrating an extended Bow-Tie model to prevent and mitigate the potential consequences of an accident and making decision and recovery. In such approach is possible to determine the probabilities of potential consequences and importance for BC updating probability

through *Bayesian Network* and perform analysis providing alternative designs for decision makers using *Constrained Goal Modelling*.

In literature are also available defined procedures for specific domains such as Electrical Infrastructure in [74] where authors highlight the added value of the Business Continuity in the IT world and how a proper operational Risk Management strategy is mandatory in order to reach an appropriate level of continuity. Their step-by-step procedure is based on ANSI 942 [75] standard which classifies four different 'Tiers':

1. Basic architecture;
2. Redundant capacity components architecture;
3. Concurrently maintainable architecture;
4. Fault tolerant architecture;

each one with specific performance levels. Following this procedure means reach an adequate operational risk management strategy to improve continuity level required in such kind of infrastructure.

ISO22301, the predecessor of BS25999-2, represents one of the most important benchmark by which professionals should be able to contribute to evaluate how organization's BCM arrangements are fit for purpose. In [76] is presented a clear vision about Business Impact Analysis and Risk Assessment highlighting how is difficult to analyse individual activities with equivalent financial impact due to complex interdependencies. However, Impact are not immediately identifiable as financial but sometimes they may have various implication in some organization than other. In these other case, it is important to understand what kind of Non-financial impacts organizations might have, including:

- Reputational damage;
- Low performance for customer service;

- Loss of accreditation or certification;
- Environmental damage;
- Reduction in corporate and social responsibility;
- Corporate governance failure.

Based on these considerations, analysing impact, identifying activities and collecting data, author shows related impact profile (that express the rate at witch the impact for each activity increases over time) in order to create a recovery timeline which can directly activate the planning process. The resulting timeline serve as a basis for a BCM.

The state of the art of Risk Assessment methodologies for Critical Infrastructure Protection is presented in JRC Technical Notes [77] by Giannopoulis, Filippini and Schimmer. Their report highlights that asses the overall risk is a complicated operation but is fundamental to identify threats, asses vulnerabilities and evaluate the impact on assets. In these methodologies it is important design a good level of 'granularity' to present fairly the reality and at the same time avoid excessive complexity. A correct cross-sectoral interdependencies model, in addition to allowing real-time architectures and cope with networked systems, is a very powerful tool that makes it clear heterogeneous behaviours due to the cascading effects.

In what follows we report some interesting approaches (see [77] [78] [79] and the references within):

- **Better Infrastructure Risk Resilience [BIRR]**

  Methodology that take into account infrastructure risk and resilience due to a variety of natural and man hazards including: Energy facilities, Transportation, Water treatment plans, Financial institution and Commercial office buildings. BIRR approach is focus on evaluating three interrelating indexes: ***VI*** *(Vulnerability Index),* ***PMI*** *(Protective*

Measure Index), ***RI*** *(Resilience Index).* Notice that, the use of common index help to compare, across various sectors, infrastructures of different nature.

- **CARVER2**

  CARVER stands for Criticality, Accessibility, Recoverability, Vulnerability, Espyability and Redundancy and take these criteria to assess the risk of a critical infrastructure asset. This approach suits well companies business continuity planing that take into account critical infrastructure as domain in order to protect human life.

- **Critical Infrastructure Modelling Simulation [CIMS]**

  A modelling and simulation framework for critical infrastructure which help operators to take decisions mostly in natural disaster scenarios. A very interesting tool able to combines geospatial information and a four dimensional (4D) environment (time-based) useful for the purpose of 'WHAT-IF' analysis.

- **Critical Infrastructure Protection Decision Support System [CIPDSS]**

  It is a risk assessment tool that take into account probability of threat, vulnerability and impact of all hazards with respect to interdependencies among 17 CI sectors. CIPDSS can estimate aggregated risk of CIs through common metrics but it cannot directly retrieve information relative to a specific infrastructure. This methodology is applicable to high level systems of infrastructures (e.g. national).

- **Critical Infrastructure Protection Modelling and Analysis [CIPMA]**

  A computer based tool to support business and government decision making for CI. CIPMA is restricted to a limited range of CI sectors like Energy, Telecommunication, Banking and Finance where GIS informations is a key element. This tool is mainly focused on: CI failure consequences, identification of specific points of failure, risk mapping, investment and mitigation strategies.

- **CommAspen**

  Is a agent-base simulation tool able to model interdependencies among electric power supply infrastructure, telecommunications and economical critical sectors as banking

and finance. CommAspen is a impact assessment tool capable to analyse a given scenario and show economic impact of communication congestion and outages.

- **DECRIS**

  Is a risk assessment methodology based on four-step procedure which consist to take into account Risk taxonomies and risk dimensions, analyse risk and vulnerability for specific events, additional analysis of identified events and finally deep analysis on selected events. DECRIS mainly focused on events identification related to Electricity, Water, Transport and ICT infrastructures.

- **Electricity Market Complex Adaptive System [EMCAS]**

  EMCAS is an electronic laboratory based on an agent-base modelling simulation for complex power systems. This tool is used to understand how external events affect operational and economic impacts on the power system. Each agent represent market participants with their own objective and decision rules. Simulation results cover economic impact on individual companies and costumer groups taking into account different scenarios.

- **EURACOM**

  A well defined methodological framework that consists of seven defined steps: Set up an holistic team with holistic view, Define the holistic scope, Define risk assessment scales, Understand the threat context, Review security/Identify vulnerabilities, Evaluate and rank the risk. This approach is design to overcome the assets limitations and allow an high level risk assessment (CI sector, counties).

- **FAIT**

  FAIT, that stands for Fast Analysis Infrastructure Tool, is based on the following concepts: interdependencies assessment, proximity of critical infrastructures, information association and economic impact. Such approach uses a system expert-defined, rule-base, object oriented interdependencies that are geographically interconnected.

This tool is designed to calculate the economic impact due to disruption of asset localized in specific region.

- **Financial System Infrastructure [FinSim]**

  Is an agent base-model simulation, specialised on financial infrastructure shall consider cash and barter transactions taking into account contractual relationships and network at federal reserve level. It may be applied on use cases in which crisis affecting the banking payment system.

- **Multilayer Infrastructure Network [MIN]**

  Multilayer Infrastructure Network is a software/methodology able to combine agent-base simulation with The Game Theory in order to generalize the paradigm of transportation network infrastructure. This approach is restricted to impact assessment.

- **Modular Dynamic Model**

  Software based on agent-base modelling and dynamic system modelling able to simulate interaction among electric infrastructure including operation of generators, transmission, distribution, energy trading and delivery of fuel to power generator. This tool is designed for CI operators and Decision Maker with a certain level of expertise.

- **NISAC Agent-Based Laboratory for Economics [N-ABLE]**

  N-ABLE is a distributed agent-base simulation, specialised on economic factors of infrastructures, with a sophisticated mathematical background on the theory of complex networks. This tool is used to identify vulnerabilities of economic sectors caused by critical infrastructure destruction.

- **Network Security Risk Assessment Model [NSRAM]**

  Network Security Risk Assessment Model (NSRAM) is a tool for Critical Infrastructure Protection based on a complex network system simulation modelling that cover all interconnected infrastructures. NSRAM is designed to analyse network behaviour where there are structural breakdowns or network faults. Such analysis supply information about system service performance through security and risk metrics.

- **RAMCAP-Plus**

  RAMCAP-Plus is an high-level risk assessment approach with the purpose to cover all critical infrastructures. This methodology is based on a seven step: Asset characterisation, Threat characterisation, Consequence analysis, Vulnerability analysis, Threat assessment, Risk and Resilience assessment and Risk an Resilience Management

Typically, Risk Management deals with the use of mathematical techniques not always able to handle the dynamic associated with the risk evolution. The main objective of the proposed framework, is to provide a flexible tool able to exceed the limits of other existing approaches, achieving a proper level of complexity. From this perspective, CISIApro represents a good solution to assess risk due to resource/fault propagation also considering cascading effects.

7.4 Proposed Framework & Architecture

Usually Risk Analysis and Business Continuity are mainly focused on prevention and consequences mitigation. In our case study a real-time performances monitoring is also considered in order to have an ongoing decision support system (DSS). Such DSS should be designed for different purposes in an organizational and strategic business continuity context. In the next sections we provides some guidelines for the implementation of a Business Continuity real-time Risk Assessment tool which may divided into the following steps:

1. **Identify & Modelling Organizational Management Structure** (or represent how competences interacts and spreading onto other people which belong to the same organization);
2. **Modelling involved Critical Infrastructures**, modelling strategical assets and identify high-priority faults (e.g. Fire, Earthquake, Flooding and so on);

3. **Identify key performance metrics/indicators**, to continuously monitor departments, and global holistic Quality of Service;
4. **Modelling Decision Support Systems** like:
    - Staff Relocation;
    - Predictive Assets Maintenance;
    - Emergency Management;
    - Disaster Recovery.

It should be noted that when we have more then one DSS is mandatory to coordinate them with a well designed '**DSS Orchestrator**' (Figure 7.2) able to activate and coordinate one or more solution supplied by the different DSSs.

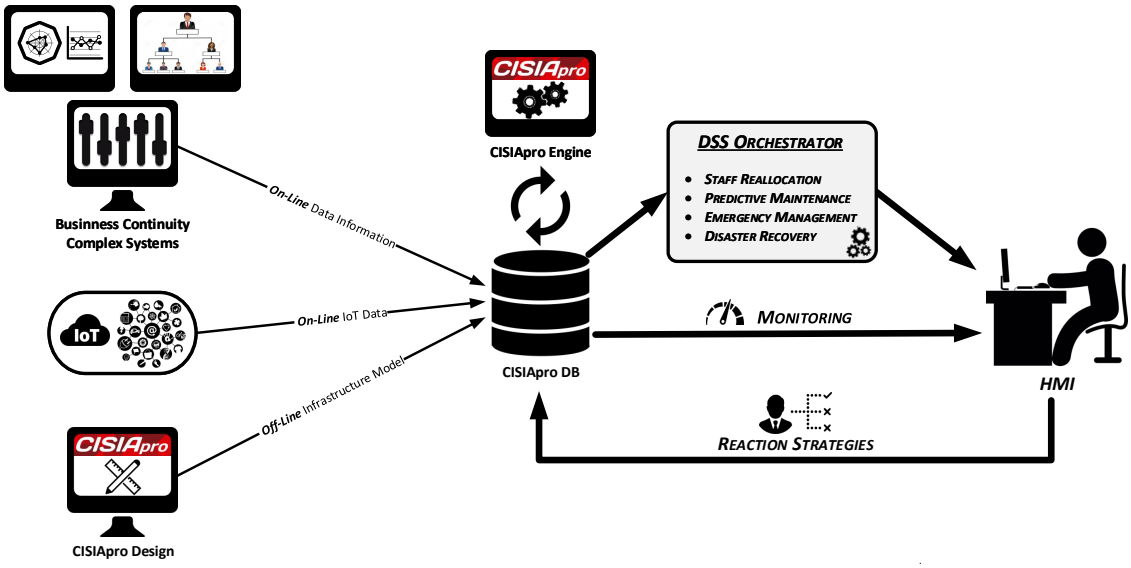


Figure 7.2 Proposed architecture.

7.5 Organizational Structure Background

There are a lot of opinions about different definitions with respect to adopted organizational structures. Walcot in [80] identifies the structure as basic aspect of the organization, including hierarchical and responsibility levels, roles, positions, integration and problem-solving mechanisms. We should not forget that business organization is integral part of complex interconnected system which includes: work environment, infrastructures providing basic services and unforeseen events. In [81] authors define organizational structures as a relatively durable distribution of work roles and administrative mechanisms to create a model of interconnected work activities that allows the organization to conduct, coordinate and control its activities. Core tasks under which an organizational structure must fulfil are basically three:

- Indicate employees relationships and hierarchical organization levels;
- Identify all individuals in organizational units and define their position within the organization;
- Design systems that guarantee coordination and communication within organization ensuring greater integration of whole efforts among organizational units.

Organizational structure is represented through an organizational chart which graphically describes hierarchical system of process and activities. In order to identify a coherent organizational model, in what follows we briefly introduce the most important organizational structures with respect to strengths/weaknesses and considered levels of management.

Hierarchical Structure - This organizational structure is based on the hierarchical principle obtaining coordination with corporate operational lines through the enhancement of the authority-dependency relationship. This model guarantees the classical

principles of direction unity, control and ensures the assignment of roles, responsibilities and internal relationships.

Functional Structure - This structure was provided by Taylor in his organizational model. Improves sectoral specialization and gives the possibility to control both targets and efficiency.

Functional-Hierarchical Structure - Modern corporation are oriented towards mixed structures like the Functional-Hierarchical. In order to be effective, such organizational structure, must design a properly sized organizational chart which meets the needs of corporate 'mission'.

Divisional Structure - It is also known as 'Product Structure', is a hierarchical decomposition of a product which brings together each organizational function into a division. Every internal division contains all required resources and functions.

Matrix Structure - This kind of structure should be preferred for medium-size organization working on products customization and operating in unstable markets. Governance of such structure requires a strong commitment through the proper management of interpersonal relationships.

Adhocratic Structure - This structure is recommended in strong innovation market scenarios. Tasks are distributed in working groups. The Adhocratic Structure adopt a double grouping. The first one is the 'Market Dimension' due to the project dimension and innovation, the second one is the 'Functional Dimension' that allows development of specialized skills and maintain a 'efficiency tension'.

The levels of management - They can be classified in three broad categories:

- Top level/Administrative level;
- Middle level/Executory;
- Low level/Supervisory/Operative/First-line managers.

Top Management includes owners/shareholders, Administrative Board, Chairmen and Sector Leaders. Middle Management consists of Managers while Low Management is composed by Senior and Junior.

7.6 Case Study

Organisational Management Structure – In order to represent a real case study we chose to design and modelling a generic Functional-Hierarchical organizational structure Figure 7.3. Such structure allows to represents and highlights hierarchical dependencies and interdependencies among units of a same department. It is important to understand that when we speak about interdependencies, we can say that like management chain is able to propagate its managerial skills downwards, improving productivity performances of individual professionals, at the same way operative resources (like Junior and Senior employees) are able to propagate their work-power upwards increasing global and sectoral productivity results. Merging representation of the Organizational Management Structure with the physical model of involved Critical Infrastructure (building and provided services like power distribution an water distribution systems) allows a real-time supervising sectoral and global performances which can suffer of significant changes due to possible cascading effects. In our case study 6 departments, 12 work units and 210 employees are modelled.

Board of Trustees - Board of Trustees and **CEO** (Chief Executive Officer) are the organ designated to company's administration. Members of Board of Trustees can be divided into three categories: Chairman, interior Administrators and external Directors.

Finance Department - Head of the department is **CFO** (Chief Finance Officer). CFO managed groups are Investor Relations (IR), Finance and Internal Audit (IA).

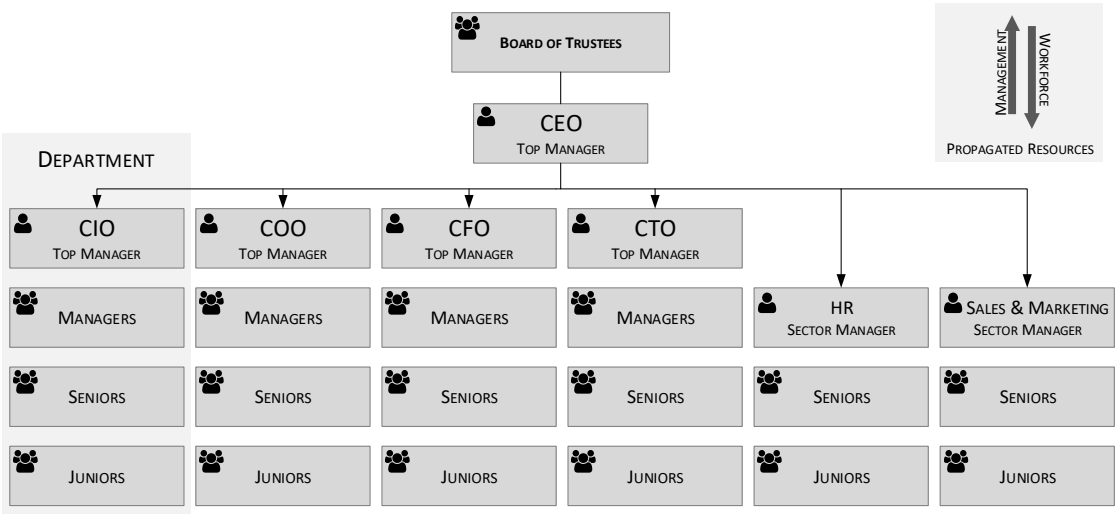


Figure 7.3 Modelled Organisational Management Structure.

Financial group is divided into groups that dealing with taxation, treasury management and accounting. IA group is divided into Financial Audit, Compliance Audit and Performance Audit groups. *Modelled department is composed by 65 employees.*

Operations Department - Head of the department is **COO** (Chief Operations Officer). COO managed groups are Project Management and Operations Management. Project Management is divided into Planners and Project Manager (PM) Staff. Operations group further subdivide logistics and commissioning of goods produced by the company. *Modelled department is composed by 37 employees.*

Information Department - Head of the department is **CIO** (Chief Information Officer). This department is divided into Customer Service group, with its Customer Care service and IT (Information Technology) group which dealing with IT Architectures. *Modelled department is composed by 25 employees.*

Technological Department - Head of the department is **CTO** (Chief technology Officer). CTO department is divided into Research and Development, Quality and Manufacturing groups. It is a strategical sector handles the market directions decreasing

uncertainty, anticipating future needs, building innovation and skills. Quality group is divided into three sub-groups: Quality Control, Quality Assurance and Documentation Control. *Modelled department is composed by 43 employees.*

Human Resource Department - In Human Resource Department sector leader is not provided because a professional like CHRO (Chief Human Resource Officer) is rarely required in medium-size organizational structure. Such sector is divided into Recruiting & Selection, Benefit & Compensation and Training & Development groups. Sector mission is Recruiting, Training and Development maximizing corporation performances through continuous improvement of available resources for the business processes. *Modelled department is composed by 14 employees.*

Marketing Department - Even in this department a sector leader is not provided. Sales Coordinator is responsible for managing sales, planning, archiving important documents and communicating relevant information. Digital Marketing has the task of maintain customers confidence towards the company. While Communication Team advertises marketing material through specific channels. *Modelled department is composed by 17 employees.*

Senior & Junior - Senior and Junior employees represent the final element of the management chain, the real workforce. In order to work on a real case study a proper identification of areas of competence and employee personal skills is necessary. Estimate correctly these values is mandatory to properly calculate performance indexes. In our framework, performances values, are indicators able to promptly trigger Decision Support Systems. Represent too much individual information can be a disadvantage because may overstrain the final interdependencies model and weigh down DSS algorithms resolution.

Therefore the decision was taken to grouping all competencies in 4-macro skills areas as suggested by enGauge 21st Century Skill Figure 7.4:

Figure 7.4 Macro Competence Areas.

- Digital-Age Literacy (Digital area);
- Inventive Thinking (Creative area);
- Effective Communication (Communication area);
- High Productivity (Productivity area).

In this way it is possible to assign each recognisable micro-skill to one macro-skill areas evaluating its weight. In Table 7.1 and Table 7.2 assigned values are summarized.

Table 7.1 4-Macro classes Senior & Junior skills evaluation.

SENIOR	Digital	Inventive	Eff.Com.	High Prod.
IR Officer	57.2%	0%	97.7%	0%
Tax Senior	42.8%	0%	30.9%	0%
Treasury Senior	42.8%	54.2%	47.6%	0%
Accounting Senior	57.4%	0%	47.6%	100%
Financial Audit	57.4%	34.2%	81.2%	0%
Compliance Audit	71.4%	34.2%	64.3%	64.2%
Performance Audit	42.8%	34.2%	97.7%	0%
Planner Senior	42.8%	34.2%	47.6%	64.2%
Project Manager	42.8%	74.2%	100%	64.2%
Supply Chain & Delivery	42.8%	54.2%	30.9%	64.2%
Commissioning	57.2%	0%	97.7%	100%
Customer Care	28.7%	74.2%	97.7%	0%
IT System Architect	43.2%	52%	79%	100%
Researcher	71.4%	100%	47.6%	64.2%
Developer	43.2%	54.2%	81%	64.2%
Quality Control	57.2%	54.2%	47.6%	64.2%
Quality Assurance	42.8%	74.2%	30.9%	0%
Document Control Centre	42.8%	34.2%	0%	64.2%
Production Senior	28.7%	34.2%	0%	64.2%
Recruiting & Selection	28.7%	34.2%	97.7%	0%
Benefit & Compensation	57.2%	34.2%	47.6%	0%
Training & Developer	28.7%	74.2%	47.6%	0%
Sales Senior	42.8%	94.2%	100%	64.2%
Digital Marketing	57.2%	74.2%	97.7%	64.2%
Marketing Communication	100%	94.2%	97.7%	0%

Infrastructure Scenario – Given the complexity of the reality, it is very hard to model every conceivable incident/event type. Adopt a risk-based approach ensure organization to adequate respond, recovery and restore any unexpected incident/emergency/crisis. To get as close as possible real complexity, an Hybrid Risk Evaluation tool is a prerequisite in order to get information of different nature, normalize them and dynamically assessing the risks. To do this we use CISIApro (Critical Infrastructure Simulation by Interdependent Agents). CISIApro is an agent-base simulation software that is able to modelling complex systems behaviours due to dependencies and interdependencies. Each agent is modelled by an entity which produce resources, fault, services and data. Starting from the proposed model by Rinaldi in [22] we are able to analyse Critical Infrastructures summarizing entities behaviours in a

Table 7.2 4-Macro classes Junior skills evaluation.

SENIOR	**Digital**	**Inventive**	**Eff.Com.**	**High Prod.**
IR Officer	57.2%	0%	97.7%	0%
IR Officers	43%	0%	83.5%	0%
Legal Specialists	28.6%	0%	16.7%	0%
Treasury Assist.	28.6%	40%	33.4%	0%
Accountant	43.2%	0%	33.4%	100%
Financial Auditors	43.2%	20%	66.8%	0%
Compliance Auditors	57.2%	20%	50.1%	50%
Performance Auditors	28.6%	20%	83.5%	0%
Planners	28.6%	20%	33.4%	50%
Project Manager Officer Assist.	28.6%	60%	100%	50%
Logistic Officers	28.6%	40%	16.7%	50%
Commissioning Officers	43%	0%	83.5%	100%
Telephone Operators	14.3%	60%	83.5%	0%
IT Technician	28.6%	40%	67%	100%
Associate Researcher	57.2%	100%	33.4%	50%
Developer Associate Specialists	28.6%	40%	66.8%	50%
Quality Control Inspectors	43%	40%	33.4%	50%
Quality Assurance Responsibilities	28.6%	60%	16.7%	0%
Document Control Centre Spec.	28.6%	20%	0%	50%
Production Technicians	14.3%	20%	0%	50%
HR Consultants	14.3%	20%	83.5%	0%
Benefit & Compensation Assist.	43%	20%	33.4%	0%
HR Assistants	14.3%	20%	33.4%	0%
Sales Coordinators	28.6%	80%	100%	50%
Digital Marketing Assistants	43%	60%	83.5%	50%
Marketing Communication Ass.	85.8%	80%	83.5%	0%

4-layers model which includes: Physical Layer, Logical Layer, Geographical Layer and Cyber Layer. During the simulation, each k-step produced in CISIApro engine take a 'snapshot' of whole system and analyse evolution of each modelled entity. When one or more events occur triggers are activated with the consequent produced cascading effects. Once CISIApro engine converge to a stable solution, risks evaluation are performed. Intuitively, in a real-time context, taking into account only the triggered entities, we are able to evaluate Operational Level (produced by CISIApro engine) as ***Risk Impact*** (RI) through a given Risk Index:

$$Risk\ Index = 1 - \ Operational\ Level \quad \in \quad \{0, 1\} \tag{7.1}$$

This RI can be useful when we need to instantiate some kind of alert thresholds in our monitoring systems. In a simulated context, we can also use this evaluated *Operational Level* as multiplicative factor to improve calculation of well known Risk Formulas like:

$$Risk = f(\ Threats \times Vulnerability \times Impact\ ) \tag{7.2}$$

On the contrary, when we take into account risk caused by specific entity, duo to cascading effects (Risk Propagation), we can use produced *Risk Index* (Formula 7.1) as dynamical multiplicative factor to calculate a real-time entity ***Risk Exposure*** (RE). This means a possible prediction concerning the current CI scenario evolutions.

In a wider perspective, modelling the building corporate headquarters, have a dual-use. On the one hand evaluating building workspaces required standards with respect to indoor environmental quality [82] (square meter needed per employee, maximum number of employees per office room, air quality, light, temperature and humidity in working environment, fire prevention indexes). On the other hand it is possible set up energy quality management systems and monitoring systems able to determine in an emergency context *Where* and *How* many people there are inside the building. Of course we must have at our disposal data that come from complex event processing systems, sensor data acquisition like IoT systems, employees badge systems and so on.

In our case study we consider a corporate building that fits the number of modelled employees. Working spaces are assigned to each organization department. Also, according to employee level, square meter have been divided in 30 sq.m. for the Chairman and for each Directors, 10 sq.m. for a Top Management, 7 sq.m. for a Sector Leader, 5 sq.m. for a Manager and finally, following standards, 2 sq.m. for each Senior and Junior employee will be assigned into the same working space. *Modelled case study count a total of 43 offices, 14 toilets and an open space of 40 working desks.* The

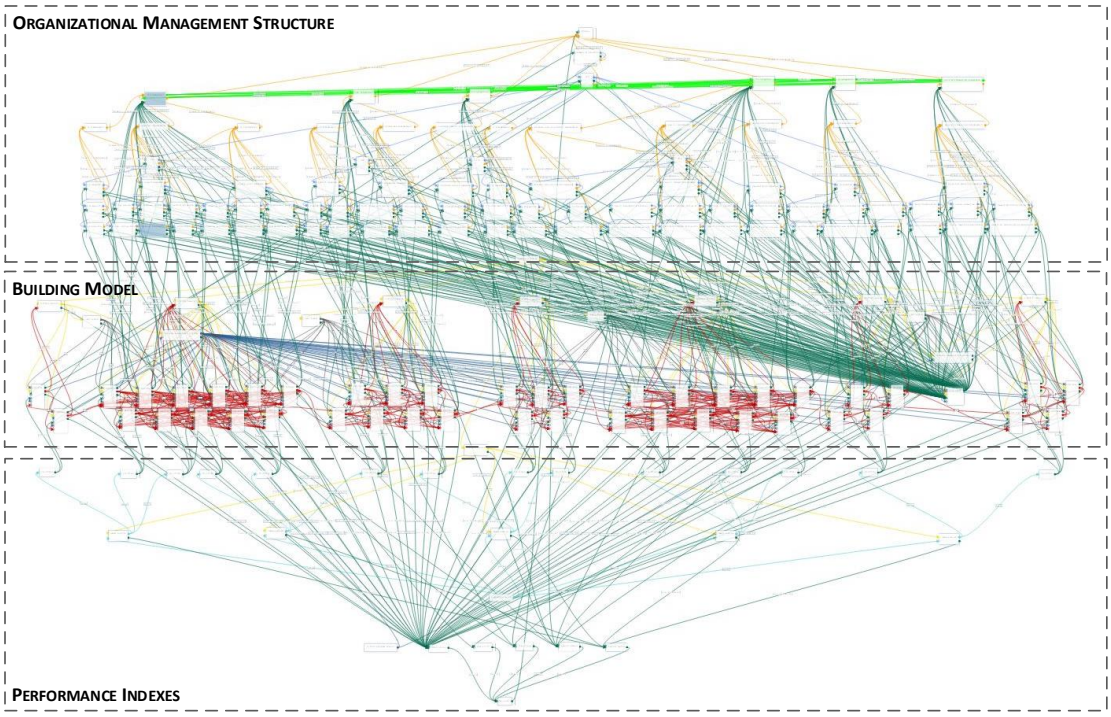


Figure 7.5 CISIApro interdependency model.

Open space is modelled because is useful in case of out of order offices but, according with [83], it brings a negative effect on their 'Operational Level'.

Taking into account building supplied services, that came from power and water distribution system, *7 electrical panels* have been introduced in the CI model considering 1 per department and 1 to supply energy for the draw pump operation. There are *5 draw pump* which have a dependency with *14 bathrooms* (each bathroom with three toilettes). In order to heating and cooling working environment the needed Kw were estimated. To meet with energy demand *heat pump* have been introduced. With regard to telecommunication there are *2 network management system.*

Another important modelled aspect is about mutual interdependencies. This concerns activities highly correlated each other. Every activity carried out by an individual, directly affect those made by other individual inside the same organization ecosystem. Formed relationships are characterized by the high level of complex

information sharing and communication. Given that cooperation takes place through tacit interactions, some logical interdependencies among organizational department were modelled. CFO department presents 3 mutual interdependencies with CIO, HR and S&M departments. The other mutual interdependencies are: 5 for the CIO department, 3 for the COO department, 4 for the CTO department, 5 for the HR department and 4 for S&M department. For Safety & Security aspects *a Fire Propagation* is considered and implemented in the corporate building model (we suppose to have this kind of data from Fire Detection System).

Following MHR modelling technique guidelines, in order to evaluate QoS of every building ecosystem, service entities are modelled. In the same way, going up with respect to CI model abstraction, global QoS through Holistic Entity were modelled. Figure 7.5 represents the described model in CISIApro interdependencies design tool.

7.7 Staff Reallocation Problem as Example of Integrated DSS

As we said, in framework introduction, Decision Support Systems that are possible design in a complex interdependences model are manifold. Usually, in CI context is common to address issues regards Disaster Recovery and Emergency Management DSS. This chapter come out from the idea to demonstrate how the versatility of proposed approach can helps in the Business Continuity field. For this reasons in this section we propose integration of a DSS which can solve the Staff Reallocation Problem. Obviously, to correctly address occurred critical situation, at given time, our system is able to switch to different DSSs thanks to risk activation thresholds. Solve a Staff Reallocation problem during a fire propagation is not advisable. In order to simplify the model only Junior employees are grouped in subsections. It should be

also noted that Reallocation Algorithm is able to move exclusively Junior employees from one group to other. At the end of the model simulation, there will be *efficient* (performance indicators with maximum values), *over-performance* (lower workload with respect to group dimensioning), *under-performance* (due to Lack of Personnel and Building Failures) and *inefficient* (higher workload with respect to group dimensioning) departments. Proposed Objective Function is designed to maximize organizational performance indexes given ***section strategic importance***, ***level of information among departments*** and ***level of services offered by company building***:

$$\max \left(\sum_{1}^{k} \left(\sum_{1}^{n} \frac{P_{nk}}{n} \times \sum_{1}^{n} \frac{I_n}{n} + Info_k \times W_{INFO} + \left(1 - \left(\sum_{1}^{n} \frac{I_n}{n} + W_{INFO} \right) \right) \times LS_k \right) \right) \times W_{DEP} + LSB \times W_{OP} \tag{7.3}$$

Where:

- k number of considered organizational department;
- n number of groups in the department;

and given variables:

- P Percentage performance;
- I Strategic importance value of n-section expressed by decimal number $\epsilon(0;1)$;
- LS_k service level supplied to k-department workforce by building work offices assigned to k-department;
- LSB total service value supplied by the building offices where $W_{OP} = 0.4$ (40% of the total weight) is the performance weight associated to office;
- $Info$ represent the modelled information sharing level value of k-department where $W_{INFO} = 0.1$ is the associated weight;

- W_{DEP}=0.1 weight associated to each department (k=6 departments with a total weight of 60%. Hence $\frac{0.6}{k} = 0.1 \rightarrow 10\%$).

$\sum_1^n P_{nk}/n \sum_1^n I_n/n$ represents the sum of departments performance taking into account their strategic importance. $(1 - (\sum_1^n I_n/n + W_{INFO}))LS_k$ represents the k-department supplied performance thanks to building supplied services.

The DSS consists of 4 phases (Figure 7.6) and each phase presents the same formulation which change only for:

Phase-1 exchange of employees between inefficient and over-performance sections

Phase-2 exchange of employees between inefficient and under-performance sections;

Phase-3 exchange of employees between under-performance and over-performance sections;

Phase-4 exchange of employees is extended to efficient groups taking into account strategic value associated to such groups.

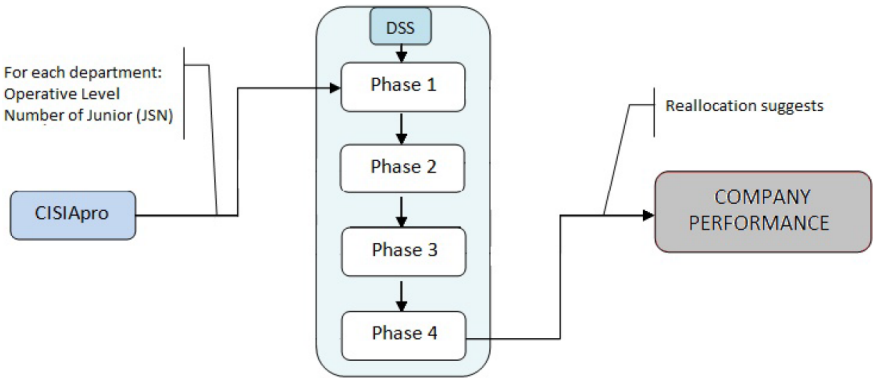


Figure 7.6 DSS process representation.

We should be noted that significant variation for each problem formulation phases are pointed out introducing 4 constraints in order to block exchange in case of strategically

less important sections. When exists the possibility to exchange resources between two sections we consider an element $a \in V_1$ and an element $b \in V_2$. We define the decisional variable y, x_i, w_i for *i=d(digital), i(inventive), ec(effective communication), hp(high productivity)*. The problem is subject to several constrains:

$$OP = \frac{1}{p}\sum_{1}^{q} OL_q \times r_k \quad \forall \ section \tag{7.4}$$

is n-group operative objective evaluation function;

$$m = \sum_{1}^{q} CD \times r \tag{7.5}$$

is the total sum n-group that take into account the total number of p employees that belong to the group;

$$OI = \frac{1}{m}\sum_{1}^{q} CD_q \times OL_q \times r_k \quad \forall \ section \tag{7.6}$$

represents the n-group individual objective evaluation function;

$$SR = \sum_{1}^{SK}\left(\frac{OP+OI}{e}r_1 + \sum_{2}^{q}\frac{OP+OI}{e}r_q w_{SK}\right) \quad \forall \ SK(SK_d, SK_i, SK_{ec}, SK_{hp}) \tag{7.7}$$

is the constrain with respect to required skills by n-group in order to have maximum performance value. In our case study we consider 4 given value of SR: $\mathrm{SR_d}$ (digital), $\mathrm{SR_i}$ (inventive), $\mathrm{SR_{ec}}$ (effective communication), $\mathrm{SR_{hp}}$ (high productivity). With SK we mean the effective Junior employees skills values that belong to n-group: $\mathrm{SK_d}$, $\mathrm{SK_i}$, $\mathrm{SK_{ec}}$, $\mathrm{SK_{hp}}$.

$$x_d + x_i + x_{ec} + x_{hp} \geq w_d + w_i + w_{ec} + w_{hp} - 1 \tag{7.8}$$

is useful to evaluate if the exchange is allowed. If the constraint is not satisfied the algorithm evaluates the next b-element, where:

$$x_i = \begin{cases} 1 \;\; IF \;\; SK_{i_a} - t \leq SK_{i_a} \leq SK_{i_a} + t \\ 0 \;\; OTHERWISE \end{cases} \tag{7.9}$$

$$w_i = \begin{cases} 1 \;\; IF \;\; SK_{i_a} \geq 0 \\ 0 \;\; OTHERWISE \end{cases} \tag{7.10}$$

for *i={d, i, ec, hp}* and t threshold to accept competence in a certain macro area. In our case study we chose $t = 0.2$ after several tests: with this value we can reallocate about 40% of employees.

$$SF_{d_a} = \left(SF_{d_a} + \left(\frac{SF_{d_a}}{JSN_{d_a}} \right) JSN_{d_b} \right) \; y \tag{7.11}$$

$$SF_{i_a} = \left(SF_{i_a} + \left(\frac{SF_{i_a}}{JSN_{i_a}} \right) JSN_{i_b} \right) \; y \tag{7.12}$$

$$SF_{ec_a} = \left(SF_{ec_a} + \left(\frac{SF_{ec_a}}{JSN_{ec_a}} \right) JSN_{ec_b} \right) \; y \tag{7.13}$$

$$SF_{hp_a} = \left(SF_{hp_a} + \left(\frac{SF_{hp_a}}{JSN_{hp_a}} \right) JSN_{hp_b} \right) \; y \tag{7.14}$$

$$SF_{d_b} = \left(SF_{d_b} + \left(\frac{SF_{d_b}}{JSN_{d_b}} \right) JSN_{d_a} \right) \; (1 - y) \tag{7.15}$$

$$SF_{i_b} = \left(SF_{i_b} + \left(\frac{SF_{i_b}}{JSN_{i_b}} \right) JSN_{i_a} \right) \; (1 - y) \tag{7.16}$$

$$SF_{ec_b} = \left(SF_{ec_b} + \left(\frac{SF_{ec_b}}{JSN_{ec_b}} \right) JSN_{ec_a} \right) \; (1 - y) \tag{7.17}$$

$$SF_{hp_b} = \left(SF_{hp_b} + \left(\frac{SF_{hp_b}}{JSN_{hp_b}} \right) JSN_{hp_a} \right) \; (1 - y) \tag{7.18}$$

$$x_d, x_i, x_{ec}, x_{hp}, w_d, w_i, w_{ec}, w_{hp}, y \in (0, 1) \tag{7.19}$$

these last eight constraints are related to the skills update due to exchanged Junior employees, JSN is surplus/necessary department Junior employees and y is linked to

allowed number of Junior employees which can be moved.

$$y = \begin{cases} 1 \;\; IF \;\; JSN_a \geq JSN_b \\ 0 \;\; OTHERWISE \end{cases} \tag{7.20}$$

7.8 Conclusion

The framework presented in this chapter shows a procedure for business continuity and risk assessment providing a valid approach for organizations that want to control their performances. The main idea, at the basis of this work, is to make evident how it is important to enhance more complexity into CI models but with a low impact on solution performances. Introducing complexity means to create a common basis for DSSs, that might work at the same time, avoiding conflicts and confusion in the supplied solutions. From this point of view is mandatory to correctly design a DSS Orchestrator able to simultaneously coordinate various DSSs.

In addition we have proposed a Staff Reallocation algorithm as example of achievable Decision Support System into such architecture. It provides possible alternatives to reallocate human resources in under-performance situations. It should be noticed that, the internal dynamics of the organization (such as the decisions at management level) can limit the use of the presented strategies. Hence, the model gives the possibility to introduce a strategic value of importance for each unit and the flexibility to add and remove units. Thresholds, to set the HR reallocations, can be changed by the operator to obtain specific percentage in the process.

In such context integrate CISIApro engine helps decision makers to evaluate the damage propagation and the CIs potential risks. This approach has been experimentally tested on a realistic and quite complex case study, through a private web-based platform.

Chapter 8

Dynamic Risk Analysis for Emergency Management

Modern society is exposed both to natural and artificial disasters related to human activity. Those same disasters can have a great impact on citizens, private and public assets. Unfortunately, as a matter of fact, it is only after losing several lives because of human errors and plans that turned out to be ineffective, that society has realized the need to improve emergency procedures introducing new solutions and instruments. Nowadays, scientific community is greatly interested in Emergency Management, and it has started to exploit the new Computer and Automation technologies involved into the Smart Cities ecosystems. Some guidelines are defined in order to design an effective Decision Support System by identifying potential emergency scenarios, including regulations referred both to the human behaviour and to the safety standards on infrastructure. Thanks to a Dynamic Risk Assessment, such a DSS can process heterogeneous data and carry out an active support for the building's evacuation procedures. The proposed architecture consists of a hybrid approach based on techniques and models of operational research and management engineering. Through this

strategy, a smart decision-making system able to provide the optimal evacuation routes from a building after the catastrophic event it was implemented.

8.1 Introduction

The exodus of people threatened by any critical event, such as a fire, is acknowledged as being key because it is aimed at ensuring the safety of people. The emergency evacuation process is very complex. Actually, being an activity conditioned by many factors it requires a thorough study: in addition to traditional factors, such as exodus routes and building's characteristics, also people psychological conditions have to be taken into account.

One of the causes that can generate panic is the incorrect preparation of a system that guarantees an adequate way of escape for the occupants. The results could be helpful in developing tools to support the building evacuation management issues. Though each situation is different there are some common aspects to all types of emergencies that involve the building evacuation. In fact, in several occasions, experience has highlighted that the onset of unsustainable critical conditions can strongly influence the occupant's exodus.

The fundamental parameters that characterize a critical situation are temperature and heat excess, evacuation routes visibility, presence of smoke, carbon monoxide and dioxide concentration. In particular, the presence of smoke affects visibility and orientation, and it makes more difficult to reach the safety exits. Low visibility must be added to the light dispersion due to smoke and the toxic effect that the components of combustion produce on the human body. For these reasons, all occupants must be able to behave properly wherever an emergency occurs.

8.2 Contributions

Main aim of such work consists in defining and developing an innovative decision-supporting system able to process the heterogeneous available data and evaluate the decision-maker preferences, typically the emergency Manager. The tool operates in buildings evacuation procedures and compartments' isolation to isolate the emergency. The resolution strategy consists of two main phases:

a) the preliminary phase, "offline", defines the building model and all the possible evacuation paths;

b) the operational phase, "online", gives - in pseudo real time - the operational suggestions, according to the detected emergencies and their development.

DSS elaborates an automated response that could speed up the evacuation process and assist Civil Protection reaction immediately after the catastrophic event onset. The pursued objectives are mainly:

a) People Protection and evacuation;

b) Assets and equipment protection;

c) Critical event confinement.

8.3 Emergency Evacuation Problem

LV, Y., et al. [84] propose an approach for Emergency Evacuation Management (EEM) based on Risk Analysis, highlighting the importance of understanding the nature of risks involved. An interval parameter joint-probabilistic integer programming (IJIP) was used to generate a range of decision alternatives, scheduling the evacuation routes

generating optimal evacuation schemes. There are several methods which deal with coefficients expressed as probability distribution, such as:

- Stochastic integer programming (SIP) – M. Branda [85];
- Fuzzy integer programming (FIP) [3] – Tan Qian, et al. [86];
- Interval integer programming (IIP) [4] – C.Z. Wu. Et al. [87].

Although the authors appreciate and identify the potential of a probabilistic-based approach, they also know limits and difficulties in implementing such techniques in complex and changeable scenarios. In fact, one of the most critical aspects is to provide a valuable Risk Assessment (RA) able to cope with the intricate patterns of the real world.

Yu, Jia, et al. [88] elaborate an approach identifiable as a simulation-based decision-making strategy, representing a complex and dynamic system, such as smart building scenarios. They propose a well-defined framework using the Multi-criteria evaluation Analytic Hierarchy Process (AHP) method. Whilst AHP is a powerful technique, it is difficult to implement it in a dynamic Real-Time information system.

Mei Yanlan and Xie Kefan [89] present a model able to select emergency evacuation strategy, in an underground station, with an approach based on triangular intuitionist fuzzy number (TIFN) and then sort the different strategies using The Elimination Et Choice Translation Reality (ELECTRE) method. Although, the authors agree with the use of ELECTRE method, TIFN could jeopardize the final results due to possible human decision-makers interaction where linguistic variables are transformed into triangular intuitionist fuzzy numbers.

8.4 Proposed Architecture

Decision Support System (DSS) usually consists of a computer system that, starting from a huge amount of data, provides useful information to increase the analysis effectiveness in a short time. It should not be considered only as a computer application, but also as a business intelligence system able to guide and support decision-making in all its aspects. The proposed solution is composed by an intelligent decision-making system that provides the optimal evacuation routes from any building sector.

Reacting to the onset of abnormal behaviour in a building, such a system proceeds to mitigate the emergency controlling fire-fighting automatic devices. It is based on a Real-Time system able to take heterogeneous data and normalize them. Thanks to a continuously updated data system a Dynamic Risk Assessment (DRA) is provided. Such DRA is automatically calculated through an agent-based simulation capable of reproducing the 'domino effect' due to modelled dependencies and interdependencies.

The output consists of a valuable amount of punctual risk metrics that represent a 'possible' near future critical scenario. Subsequently, an Expert System ELECTRE-based ranks the optimal emergency paths from each sector to emergency exits. In particular:

- **CISIApro Engine** is a hybrid validation tool that performs data fusion, collecting information from different SCADA systems and from additional data sources. With CISIApro it is possible to understand the consequences of negative events, such as failures, natural disasters or cyber-attacks. This module is crucial to the risk prediction as an assessment of the anomalous events propagation and the potential damage that could affect critical infrastructures.

- **Expert System**, based on optimization algorithms and multi-criteria methods, provides evacuation routes from every building sector, according to the emer-

gencies onset and their expected development. The Expert System uses data provided by CISIApro and it processes an optimum response to face the particular emergency scenario.

In this work we define an efficient decision-making tool, adaptable to many situations and able to provide strategic information. In the developed DSS six decision-making phases can be distinguished:

1. Building model design;
2. All possible evacuation paths definition;
3. Emergency localization, recognition and dimensioning;
4. Event risk propagation;
5. Sectors integrity analysis;
6. Evacuation paths identification.

Expert System – Minimum path – Minimal path search problem has been addressed using graph-based representation. Given a not-oriented graph $\mathcal{G} = (V, E)$, at each arc $e = (u, v) \in E$ is associated a weight $p_{u,v} \in R$. For each oriented path it is possible to define the weight $p(P)$ of path p as the sum of the arcs' weights belonging to P:

$$p(P) = \sum_{(u,v)\in P} p_{(u,v)} \tag{8.1}$$

The problem can be expressed as follow: *Given two nodes $u \in V$ and $v \in V$, the problem is to find an oriented path $P^*(u, v)$ in G from u to v that has minimum weight.* Dijkstra algorithm allows to solve the minimum path problem between two nodes in case all the arcs weights are not negative. The authors chose this algorithm because

it achieves a better computational complexity than many other analysed strategies. Thanks to this approach they calculate all the possible evacuation routes from every office.

CISIApro – Dynamic Risk Assessment – Typically, the Risk Assessment (RA) is associated to a cumbersome process that starts from a complex Risk Analysis passing through the involvement of 'domain' experts. Most of the time, such a process provides static tools unable to cope with the real needs in specific critical situations. This is precisely why the authors adopt a dynamic risk-based approach. This technique has been used and validated in several European Projects. Implementing a Dynamic Risk Assessment (DRA) means having a real-time agent-based simulation able to assess the risk due to 'possible' cascading effects. With CISIApro software, authors model the building case study and introduce Risk Metrics according to fire propagation in an indoor environment.

Expert System – Multi-criteria decision method – ELECTRE family methods implement the Pareto optimum concept as a decision-making rule and create ordered alternatives according to different criteria. They identify the optimal Pareto alternatives that are not dominated by others. Such algorithm selects the most efficient compromise using the preference information provided by the decision maker. The second version of these methodologies, ELECTRE II, introduces four threshold values to increase the level of information and make more informed choices. Some correspondences must be considered. The alternatives represent the evacuation routes and they are enhanced by the criteria suggested by the decisor. Criteria identification realizes a mush up between:

- *Real information* obtainable through an environmental monitoring system;

- *Plausible information* concerning the event propagation, in the near future, prepared by risk predictor.

8.5 Problem Formulation

Planned stages to be applied are described above.

Preliminary Stage 1 – Referring to the building planimetry, a non-oriented and connected graph is generated. Edges represent sectors and arcs give the 'possibility' of moving from one sector to another. Dijkstra algorithm is applied to obtain the minimum paths from source nodes to reach end nodes. The evacuation routes are defined in accordance with the Emergency Management Plan developed for the specific building.

Input: E set of building sectors, and graph $G(S, T, P, A)$:

- $S \subset E$ set of offices;
- $T \subset E$ set of corridors;
- $P \subset E$ set of exits;
- A set of arcs according to the building planimetry.

Output: Evacuation paths and sectors that compose them.

Procedure: Dijkstra algorithm is applied to graph $G(S, T, P, A)$ to identify the optimal path from each office, in terms of distance.

Preliminary Stage 2 – Each path is considered as a sectors sequence characterized by some fundamental parameters such as integrity. Similarly, evacuation paths can be

valued by aggregating information about parameters from each sector that belongs to the path.

Input: building planimetry and data acquired from field.

Output:

- *Fire propagation index* in sector;
- *Fire Risk index* characterised by sector's position and isolation.

Procedure: Round table is made. Close collaboration with experts allows to define a plausible indoor behaviour of fire.

On-Line Stage 1 – DSS proceeds to identify the alarm level in each sector, comparing the event intensity level with predetermined values called event status threshold values, defined in accordance with the Civil Protection states of activation. Magnitude valorisation is obtained by CISIApro. Each alarm level corresponds to an intervention standard. Countermeasures, fire doors closing and fire-fighting water devices opening, are activated.

Input:

- s building sectors;
- $event\_value_i$ = fire rate of sector i $(i = 1, \cdots, s)$;
- *threshold values*: attention, warning, alarm, emergency;
- Available fire-fighting actuations.

Output: Alarms type and level for each sector involved, fire-fighting countermeasures to implement.

Procedure: $event\_value_i$ is compared to threshold values to define the sector state. Procedure is repeated for each sector.

On-Line Stage 2 – CISIApro engine, defined as *Hybrid Evaluation Tool*, gets information of data systems, normalize them and dynamically produces a risk assessment. Thanks to its features, CISIApro estimates the impact according to '*triggered entities*' (fire or gas sensors) and possible *Risk Exposure* due to modelled interdependencies.

Input:

- building sector;
- Fire sensor data;
- Fire door state.

Output: Dynamic Risk Evaluation over the building.

Procedure: Using a particular propagation rule that considers complex cascading effects, CISIApro defines the Operational Level of an entity. It represents the entity ability to produce defined level of resources depending on the availability of received resources, on the propagation of faults and on the functionality of the entity itself. Using specific inverse proportionality relationships with the operational level, CISIApro evaluates the Risk Impact and Risk Exposure Indexes for each triggered entity.

On-Line Stage 3 – DSS defines sector integrity as the weighted sum of measures derived from the Risk Predictor:

$$i_{int} = 0,5 \cdot fire\_event\_value + 0,5 fire\_risk\_value \tag{8.2}$$

Index of each sector is compared with the event threshold values to determine the integrity level. Each level corresponds to an emergency evacuation standard.

Input:

- s building sectors;

- i_{int_i} = sector's structural integrity ($i = 1, \cdots, s$);
- threshold values: attention, warning, alarm, emergency;
- Evacuation Standard.

Output: Each sector integrity and its sorting according to decreasing indexes.
Procedure: DSS establishes the sector structural integrity to identify all sectors' state. After that, sectors are ordered by decreasing integrity index to facilitate the evacuation starting from most compromised sectors.

On-Line Stage 4 – DSS identifies the best exodus routes from each sector. The aim is to minimize the time required to complete evacuation operations, using routes that have a *lower risk index*. The sectors belonging to the chosen route increase their crowd index according to the number of people expected. The algorithm defines an alternative/criteria matrix, whose elements represent the alternatives' enhancement based on each criterion.

- s' sectors to evacuate $\subset s$ building sectors;
- p alternatives (evacuation paths)
- c criteria valued for each path:
  - Lighting (maximize);
  - CO_2 concentration (minimize);
  - Smoke presence (minimize);
  - Occupants number (minimize);
  - Fire Rate Index (minimize);
  - Fire Risk Index (minimize);

  - Monitorability (minimize);
  - Distance (minimize);

- Threshold values: weak/strong concordance and discordance.

Output: Optimal evacuation paths, from occupied sector.

Procedure: following the sectors order, according to increasing values of i_{int_i}, algorithm considers each occupied source sector and applies the ELECTRE II algorithm. The first classified alternative will be suggested.

An innovative aspect of proposed architecture concerns the capability of auto-generating all the values needed to fill the Alternatives/Criteria matrixes required by ELECTRE II. Following this approach, it is possible to speed up the entire process, leading computational time below the second.

8.6 Case Study

It is provided a case study very similar to reality considering a single floor of a company where work offices, rendezvous points, emergency exits and corridors are located. However, thanks to its flexibility, this approach can be easily extended to different infrastructures, hospitals and malls. The faced scenario considers building offices involved in a seismic event that causes structural damages to E5 and fire in R2 due to a short-circuit in the electrical panel (Figure 8.1).

Figure 8.1 Floor planimetry.

Sectors are characterized by different measures (Table 8.1) :

Table 8.1 Considered measures.

Measures	Description
$Crow$	Maximum expected crowding
$Light$	Lighting value
$Smoke$	Fire smoke presence
T_SC	Toxic substances concentration
F_r	Fire Propagation Risk Index (event risk)
F_s	Fire Status Index (event rate)
M	Sector Monitorability

The correspondence between the alarm level defined for each sector and the possible countermeasures to be implemented is outlined in the Table 8.2.

Table 8.2 State/Countermeasures.

Measures	Description
Normal state	No actions
Attention state	Light signals with LED
Warning state	Light signals with LED and acoustic signalling via siren
Alarm state	As previous, plus fire doors automatic closure, if present
Emergency state	As previous, plus fire-fighting devices activation

8.7 Results

In this section obtained results by applying the elaborated strategy on the above-mentioned scenario are showed. In order to highlight the framework behaviour, simulation considers three occupied rooms **O6**, **O9**, and **O14**.

Offline stage – Starting from the floor planimetry (Figure 8.1) e coherent model is implemented with CISIApro software (Figure 8.2) and than a graph $G(S, T, P, A)$ is generated(Figure 8.3).

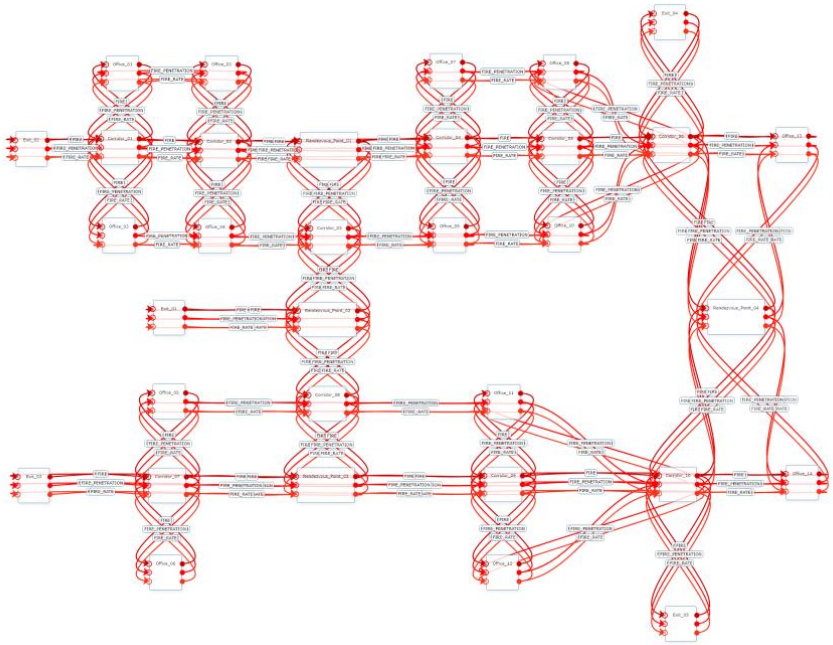


Figure 8.2 CISIApro model.

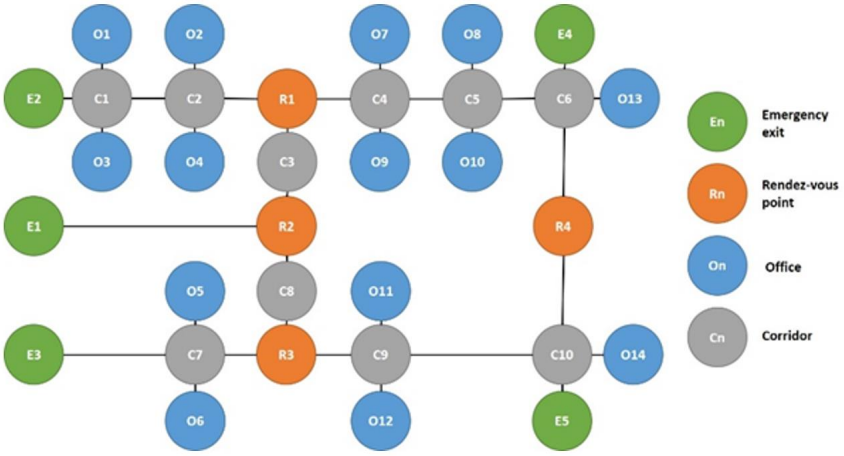


Figure 8.3 G graph.

A variation of the Dijkstra algorithm is applied, obtaining paths in Table 8.3.

Table 8.3 Evacuation routes.

Path	O6	O9	O14
1	O6, C7, EE3	O9, C4, RP1,C2, C1, EE2	O14, C10, EE5
2	O6, C7, RP3, C8, RP2, EE1	O9, C4, RP1, C3, RP2, EE1	O14, C10, C9, RP3, C7, EE3
3	O6, C7, RP3, C8, RP2, C3, RP1, C2, C1, EE2	O9, C4, RP1, C3, RP2, C8, RP3, C7, EE3	O14, C10, C9, RP3, C8, RP2, EE1
4	O6, C7, RP3, C8, RP2, C3, RP1, C4, C5, C6, EE4	O9, C4, RP1, C3, RP2, C8, RP3, C9, C10, EE5	O14, C10, C9, RP3, C8, RP2, C3, RP1, C2, C1, EE2
5	O6, C7, RP3, C8, RP2, C3, RP1, C4, C5, C6, RP4, C10, EE5	O9, C4, RP1, C3, RP2, C8, RP3, C9, C10, RP4, C6, EE4	O14, C10, C9, RP3, C8, RP2, C3, RP1, C4, C5, C6, EE4
6	O6, C7, RP3, C9, C10, EE5	O9, C4, C5, C6, EE4	O14, C10, R4, C6, EE4
7	O6, C7, RP3, C9, C10, RP4, C6, EE4	O9, C4, C5, C6, RP4, C10, EE5	O14, C10, R4, C6, C5, C4, RP1, C2, C1, EE2
8	O6, C7, RP3, C9, C10, RP4, C6, C5, C4, RP1, C2, C1, EE2	O9, C4, C5, C6, RP4, C10, C9, RP3, C7, EE3	O14, C10, R4, C6, C5, C4, RP1, C3, RP2, EE1
9	O6, C7, RP3, C9, C10, RP4, C6, C5, C4, RP1, C3, RP2, EE1	O9, C4, C5, C6, RP4, C10, C9, RP3, C8, RP2, EE1	O14, C10, R4, C6, C5, C4, RP1, C3, RP2, C8, RP3, C7, EE3

Emergency localization – After a first evaluation of the Risk Predictor, all sectors are affected by the event. Table 8.4 shows the status and countermeasures to be applied.

Table 8.4 Countermeasures suggested.

State	Sector	Countermeasure
Attention	E2	Light signals with LED
Warning	O6, O14, C1, C2, C4, C5, C6, C7, C9, C10, R4, E3	Light signals with LED and acoustic signalling via siren
Emergency	O9, R1, R3	As previous, plus fire doors automatic closure, if present

Risk propagation – Risk Predictor simulates fire propagation, this time considering the mitigation due to the countermeasures: Fire doors isolate fire and automatic water devices decrease fire magnitude. At the end of this phase, the Expert System acquires all the information necessary to process its answer, Figure 8.4.

Integrity analysis – Integrity index of each sector is calculated to determine the evacuation urgency (Table 8.5).

Table 8.5 Evacuation order.

Sector	i_{int}	Evacuation Order
O6	0,33	2
09	0,52	1
O14	0,31	3

Exodus routes identification – Each evacuation route is valued considering its sector composition according to the different criteria. The weight array expresses decision maker's preferences, $w = \{0.25, 0.25, 0.25, 0.25, 1, 0.25, 1, 1\}$. The results of **O9** and **O6** sectors are omitted, as trivial, while results related to sector **O14** are shown being more interesting.

Sector	Lumen	CO^2	Smoke	Overcrowding	Fire Rate	Fire Risk	Integrity	Monitorability
O1	400	700	NO	0	0,33 | **0,33**	0,33 | **0,21**	0,27	YES
O2	400	700	NO	0	0,41 | **0,41**	0,41 | **0,26**	0,54	YES
O3	400	700	NO	0	0,51 | **0,51**	0,33 | **0,21**	0,36	YES
O4	400	700	NO	0	0,64 | **0,64**	0,41 | **0,40**	0,52	YES
O5	400	700	NO	0	0,64 | **0,64**	0,41 | **0,40**	0,52	YES
O6	600	1000	NO	**3**	0,41 | **0,41**	0,41 | **0,26**	0,33	YES
O7	400	700	NO	0	0,41 | **0,41**	0,41 | **0,26**	0,33	YES
O8	400	700	NO	0	0,33 | **0,33**	0,33 | **0,21**	0,27	YES
O9	600	850	NO	**2**	0,64 | **0,64**	0,41 | **0,40**	0,52	YES
O10	400	700	NO	0	0,51 | **0,51**	0,33 | **0,21**	0,36	YES
O11	400	700	NO	0	0,64 | **0,64**	0,41 | **0,40**	0,52	YES
O12	400	700	NO	0	0,41 | **0,41**	0,41 | **0,26**	0,33	YES
O13	400	700	NO	0	0,33 | **0,33**	0,26 | **0,17**	0,25	YES
O14	700	1200	NO	**10**	0,41 | **0,41**	0,33 | **0,21**	0,31	YES
C1	350	2500	NO	0	0,41 | **0,41**	0,41 | **0,26**	0,33	YES
C2	350	2500	NO	0	0,51 | **0,51**	0,51 | **0,32**	0,41	YES
C3	150	4500	**YES**	0	0,80 | **0,70**	0,80 | **0,70**	0,7	YES
C4	350	2500	NO	0	0,51 | **0,51**	0,51 | **0,32**	0,41	YES
C5	350	2500	NO	0	0,41 | **0,41**	0,41 | **0,26**	0,33	YES
C6	400	1500	NO	0	0,41 | **0,41**	0,33 | **0,21**	0,31	YES
C7	350	2500	NO	0	0,51 | **0,51**	0,51 | **0,32**	0,41	YES
C8	150	4500	**YES**	0	0,80 | **0,70**	0,80 | **0,70**	0,7	YES
C9	350	2500	NO	0	0,51 | **0,51**	0,51 | **0,32**	0,41	YES
C10	400	1500	NO	0	0,51 | **0,51**	0,41 | **0,26**	0,38	YES
R1	200	4000	**YES**	0	0,64 | **0,64**	0,64 | **0,40**	0,52	YES
R2	100	5000	**YES**	0	1 | **0,90**	1 | **0,90**	0,9	YES
R3	200	4000	**YES**	0	0,64 | **0,64**	0,64 | **0,40**	0,52	YES
R4	400	700	NO	0	0,41 | **0,41**	0,33 | **0,21**	0,31	YES
E1	400	700	NO	0	0,80 | **0,70**	0,80 | **0,70**	0,7	YES
E2	400	700	NO	0	0,33 | **0,33**	0,33 | **0,21**	0,27	YES
E3	400	700	NO	0 | 3 *(step 2)*	0,41 | **0,41**	0,41 | **0,26**	0,33	YES
E4	400	700	NO	0 | 2 *(step 1)*	0,33 | **0,33**	0,26 | **0,17**	0,25	YES
E5	100	700	NO	0	0,41 | **0,41**	0,33 | **0,21**	0,31	**NO**

Figure 8.4 Criteria evaluation.

- The path from O9 sector to the emergency exit E2 is shorter but also riskier. It crosses R1, close to sectors in alarm, and it has closed fire doors that slowdown the evacuation. The optimal route suggested is n°6 to E4.
- The closest and safest exit from the O6 room is E3. So, evacuation route suggested is n°1.
- For the O14 sector the alternative/criterion matrix is in Table 8.6

Table 8.6 Evacuation order.

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**
A1	400	1133	0	10	0,44	0,22	0	7,5
A2	400	1133	0	10	0,44	0,22	0	7,5
A3	328	2771	3	10	0,62	0,50	1	19,5
A4	304	2990	5	10	0,57	0,42	1	29
A5	312	2867	5	12	0,55	0,40	1	34
A6	460	1120	0	12	0,41	0,21	1	20,5
A7	390	1960	1	10	0,45	0,27	1	29
A8	345	2410	3	10	0,56	0,42	1	30,5
A9	319	2700	5	13	0,55	0,40	1	40

The closest exit to the O14 sector is E5 but it is condemned. The second exit considered in terms of distance is E3, but it is riskier and it crosses R3 which is near the sectors in alarm. In addition to having some fire doors closed, the route is also used by the three people who evacuate from the O6 room. Instead, the E4 exit is more longer, few meters, but less risky and crowded. For these reasons the evacuation route is n°6 to E4.

8.8 Conclusion

During an emergency evacuation from a building struck by the flames, choose the safest exodus way is an example of a decision that must be taken as soon as possible. Any

uncertainties or wrong decisions can cause confusion and panic among the occupants, a situation that can easily result in rescue delays and, in the worst case, in loss of human lives. The Evacuation Management strategy proposed in this work consists in the interaction between two main modules, the Risk Predictor and the Expert System, capable of collecting, integrating and processing data from heterogeneous sources, i.e. sensors and decision maker opinions. Decision-maker plays a crucial role because of it intervenes in the criteria weights definition. Weights attach a level of importance to each criterion according to the decision maker's preferences and their variation can lead the process to different solutions.

Main objective is to manage a fire onset in a building and to intervene punctually, in particular:

- Identify, localize and indicate flames presence;
- Implement the correct countermeasures to isolate outbreaks and attenuate their intensity;
- Provide and report optimal evacuation routes.

This information can be also made available to civil protection or firefighters to better manage their resources during the operation. Case study foresees the simultaneous presence of a fire and a structural failure that made unusable two of the five emergency exits. At a preliminary stage of design and information collection for the building model definition, follows an online stage that, immediately after the anomalous event detection, elaborates a plan of actuations, as luminous and acoustic signals, fire doors closing, fire-fighting water system activation. As expected, the DSS's response provides for the activation of firefighting countermeasures in the areas affected by the event, and suggests to the occupants the safest exodus routes to the accessible emergency exits.

Over this case study, framework has been tested on a wide range of multi-emergence scenarios, always producing excellent results, both in terms of computational time during processing, and in terms of suggested countermeasures effectiveness. Thanks to its modularity and scalability, the DSS can be easily customized for any indoor reality, such as hospitals, offices, universities, etc. Connecting the DSS to an active supervision and control system active on a real building would be useful for refining the instrument and evaluating its goodness even in a real and complex situation. Known the topic's importance, we are currently engaged in the development of an autonomous decision support system able to manage the process with the minimum intervention by the operator.

The framework can be improved by defining and introducing more detailed assessments of fire physics and flame propagation in an indoor environment. In addition, expanding the management process to a multi-floor evacuation would increase the completeness of the DSS. However, at present, it creates a good compromise between huge amount of heterogeneous data acquired and computational time used to reach the solution.

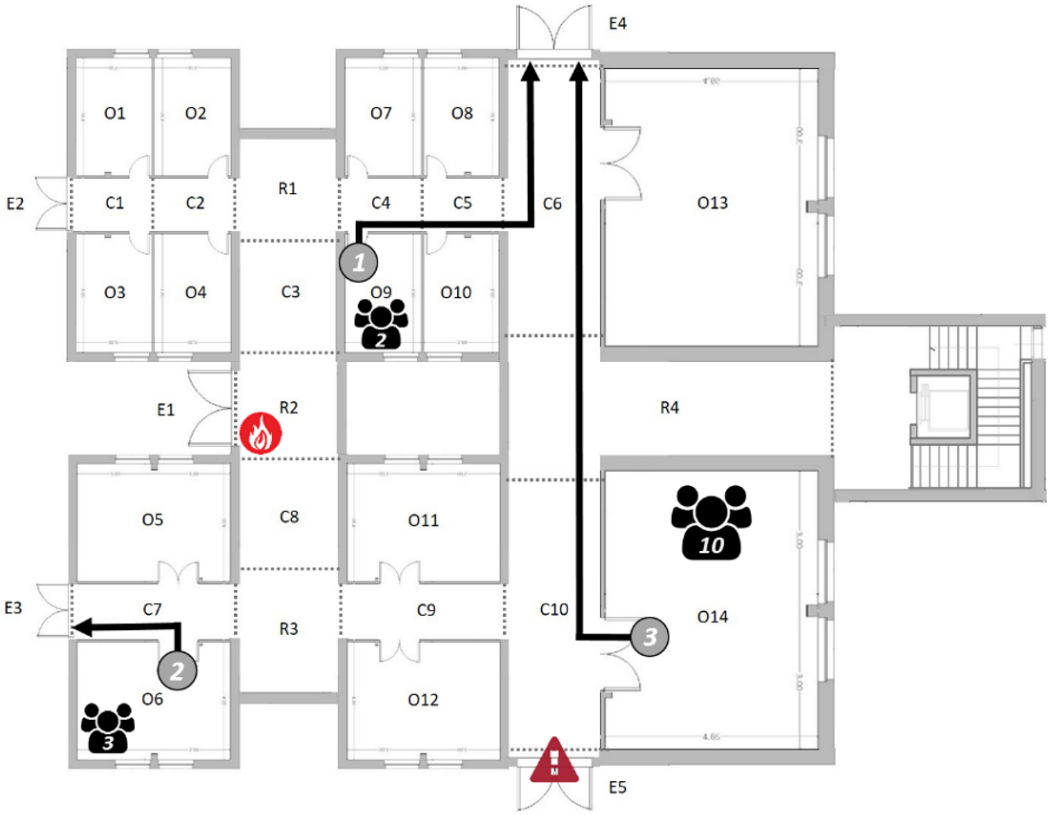


Figure 8.5 Emergency evacuation plan.

Bibliography, Publications & Deliverable

[1] G. W. Coffey, "Holistic and reductionist approaches," *A Systems Approach to Leadership*, pp. 43–52, 2009.

[2] UNISDR, *Terminology on disaster risk reduction.* UNISDR Geneva, 2009.

[3] ——, *Proposed Updated Terminology on Disaster Risk Reduction: A Technical Review*, 2015.

[4] T. Aven and O. Renn, "On risk defined as an event where the outcome is uncertain," *Journal of Risk Research*, vol. 12, no. 1, pp. 1–11, 2009.

[5] Willis and H. H, "Guiding resource allocations based on terrorism risk," *Risk Analysis: An International Journal*, vol. 27, no. 3, pp. 597–606, 2007.

[6] S. Campbell, "Determining overall risk," *Journal of Risk Research*, vol. 8, no. 7-8, pp. 569–581, 2005.

[7] Graham, J. D, Wiener, J. Baert, Sunstein, C. R *et al.*, *Risk vs. risk.* Harvard University Press, 1995.

[8] W. W. Lawrence, "Of acceptable risk," *William Kaufmann, Los Altos, CA*, 1976.

[9] ISO-2002, *Risk management vocabulary. ISO/IEC Guide 73. Geneva: ISO.* ISO, 2002.

[10] S. Kaplan and B. Garrick, "On the quantitative definition of risk," vol. 1, no. 1, pp. 11–27, 1981.

[11] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," *Reliability engineering & System safety*, vol. 92, no. 6, pp. 745–754, 2007.

[12] Cabinet_Office, "Risk: Improving government's capability to handle risk and uncertainty," 2002.

[13] E. A. Rosa, "Metatheoretical foundations for post-normal risk," *Journal of risk research*, vol. 1, no. 1, pp. 15–44, 1998.

[14] O. Renn, "White paper on risk governance: Toward an integrative framework," pp. 3–73, 2008.

[15] *ISO 31000:2009, Risk Management - Principles and guidelines*, 2009.

[16] *ISO Guide 73, Risk Management - Vocabulary*, 2009.

[17] G. and C. Merriam, "Webster's revised unabridged dictionary," 1913.

[18] L. A. Zadeh, "Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic," *Fuzzy sets and systems*, vol. 90, no. 2, pp. 111–127, 1997.

[19] T. Mass, S. O'Neil, and J. Rollins, "The department of homeland security's risk assessment methodology: Evolution, issues, and options for congress - crs report no. rl33858," 2007.

[20] M. Rausand, *Risk assessment: theory, methods, and applications*. John Wiley & Sons, 2013, vol. 115.

[21] UNISDR, "Exposure and vulnerability (short concept note: Work stream 2, working group 2)," 2016.

[22] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, 2001.

[23] S. De Porcellinis, S. Panzieri, and R. Setola, "Modelling critical infrastructure via a mixed holistic reductionistic approach," *International journal of critical infrastructures*, vol. 5, no. 1-2, pp. 86–99, 2009.

[24] C. Di Mauro, S. Bouchon, C. Logtmeijer, R. Pride, T. Hartung, and J.-P. Nordvik, "A structured approach to identifying european critical infrastructures," *International Journal of Critical Infrastructures*, vol. 6, no. 3, pp. 277–292, 2010.

[25] S. De Porcellinis, R. Setola, S. Panzieri, and G. Ulivi, "An agent based simulator for critical interdependent infrastructures." *Proc. 2nd International Conference on Critical Infrastructures, October 24-27, 2004*.

[26] D. Porcellinis, Setola, Panzieri, and Ulivi, "Simulation of heterogeneous and interdependent critical infrastructures," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 110–128, 2008.

[27] C. Foglietta, C. Palazzo, R. Santini, and S. Panzieri, "Assessing cyber risk using the cisiapro simulator," in *International Conference on Critical Infrastructure Protection*. Springer, 2015, pp. 315–331.

[28] G. Satumtira and L. Dueñas-Osorio, "Synthesis of modeling and simulation methods on critical infrastructure interdependencies research," in *Sustainable and resilient critical infrastructure systems*. Springer, 2010, pp. 1–51.

[29] H. A. Rahman, M. Armstrong, D. Mao, and J. R. Marti, "I2sim: A matrix-partition based framework for critical infrastructure interdependencies simulation," in *Electric Power Conference, 2008. EPEC 2008. IEEE Canada*. IEEE, 2008, pp. 1–8.

[30] A. Nieuwenhuijs, H. Luiijf, and M. Klaver, "Modeling critical infrastructure dependencies," in *IFIP International Federation for Information Processing*, vol. 290, 2008, pp. 205–214.

[31] S. Schütte, S. Scherfke, and M. Tröschel, "Mosaik: A framework for modular simulation of active components in smart grids," in *Smart Grid Modeling and Simulation (SGMS), 2011 IEEE First International Workshop on*. IEEE, 2011, pp. 55–60.

[32] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca *et al.*, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, 2005.

[33] A. Kwasinski, P. L. Chapman, P. Krein, W. Weaver *et al.*, "Hurricane katrina: damage assessment of power infrastructure for distribution, telecommunication, and backup." *Grainger Center for Electric Machinery and Electromechanics. Technical Report.*, 2006.

[34] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[35] A. Lemay, J. Fernandez, and S. Knight, "Modelling physical impact of cyber attacks," in *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2014 Workshop on*. IEEE, 2014, pp. 1–6.

[36] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical smart grid infrastructures," in *Innovative smart grid technologies conference (ISGT), 2014 IEEE PES*. IEEE, 2014, pp. 1–5.

[37] G. Dondossola, F. Garrone, and J. Szanto, "Cyber risk assessment of power control systems—a metrics weighed by attack experiments," in *Power and Energy Society General Meeting, 2011 IEEE*. IEEE, 2011, pp. 1–9.

[38] R. Santini, C. Foglietta, and S. Panzieri, "Evidence theory for cyber-physical systems," in *International Conference on Critical Infrastructure Protection*. Springer, 2014, pp. 95–109.

[39] E. Ciancamerla, C. Foglietta, D. Lefevre, M. Minichino, L. Lev, and Y. Shneck, "Discrete event simulation of qos of a scada system interconnecting a power grid and a telco network," in *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*. Springer, 2010, pp. 350–362.

[40] R. Zimmerman, "Decision-making and the vulnerability of interdependent critical infrastructure," in *Systems, Man and Cybernetics, 2004 IEEE International Conference on*, vol. 5. IEEE, 2004, pp. 4059–4063.

[41] K.-S. Lim and D.-R. Lee, "The spatial mcda approach for evaluating flood damage reduction alternatives," *KSCE Journal of Civil Engineering*, vol. 13, no. 5, pp. 359–369, 2009.

[42] K.-C. Shim, D. G. Fontane, and J. W. Labadie, "Spatial decision support system for integrated river basin flood control," *Journal of Water Resources Planning and Management*, vol. 128, no. 3, pp. 190–201, 2002.

[43] J. Geldermann, V. Bertsch, M. Treitz, S. French, K. N. Papamichail, and R. P. Hämäläinen, "Multi-criteria decision support and evaluation of strategies for nuclear remediation management," *Omega*, vol. 37, no. 1, pp. 238–251, 2009.

[44] R. P. Hämäläinen, M. R. Lindstedt, and K. Sinkko, "Multiattribute risk analysis in nuclear emergency management," *Risk Analysis*, vol. 20, no. 4, pp. 455–468, 2000.

[45] V. Rosato, A. Di Pietro, A. Tofani, and E. Pascucci, "The mimesis project: A decision support system for risk analysis and the impact evaluation of crisis scenarios of critical infrastructures deriving from extreme natural events," in *Electrical and Computer Engineering (CCECE), 2011 24th Canadian Conference on*. IEEE, 2011, pp. 001 523–001 526.

[46] Y. Peng, Y. Zhang, Y. Tang, and S. Li, "An incident information management framework based on data integration, data mining, and multi-criteria decision making," *Decision Support Systems*, vol. 51, no. 2, pp. 316–327, 2011.

[47] D. Ergu, G. Kou, Y. Shi, and Y. Shi, "Analytic network process in risk assessment and decision analysis," *Computers & Operations Research*, vol. 42, pp. 58–74, 2014.

[48] C.-L. Hwang and K. Yoon, "Methods for multiple attribute decision making," in *Multiple attribute decision making*. Springer, 1981, pp. 58–191.

[49] J. Figueira, V. Mousseau, and B. Roy, "Electre methods," in *Multiple criteria decision analysis: State of the art surveys*. Springer, 2005, pp. 133–153.

[50] S. Martello, "Knapsack problems: algorithms and computer implementations," *Wiley-Interscience series in discrete mathematics and optimiza tion*, 1990.

[51] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Transactions on Power delivery*, vol. 4, no. 2, pp. 1401–1407, 1989.

[52] D. Shirmohammadi and H. W. Hong, "Reconfiguration of electric distribution networks for resistive line losses reduction," *IEEE Transactions on Power Delivery*, vol. 4, no. 2, pp. 1492–1498, 1989.

[53] Q. Zhou, D. Shirmohammadi, and W.-H. Liu, "Distribution feeder reconfiguration for service restoration and load balancing," *IEEE Transactions on Power Systems*, vol. 12, no. 2, pp. 724–729, 1997.

[54] E. M. Carreno, R. Romero, and A. Padilha-Feltrin, "An efficient codification to solve distribution network reconfiguration for loss reduction problem," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1542–1551, 2008.

[55] A. B. Morton and I. M. Mareels, "An efficient brute-force solution to the network reconfiguration problem," *IEEE Transactions on Power Delivery*, vol. 15, no. 3, pp. 996–1000, 2000.

[56] R. J. Sarfi, M. Salama, and A. Chikhani, "A survey of the state of the art in distribution system reconfiguration for system loss reduction," *Electric Power Systems Research*, vol. 31, no. 1, pp. 61–70, 1994.

[57] D. Das, "Reconfiguration of distribution system using fuzzy multi-objective approach," *International Journal of Electrical Power & Energy Systems*, vol. 28, no. 5, pp. 331–338, 2006.

[58] D. P. Bernardon, V. J. Garcia, A. S. Q. Ferreira, and L. N. Canha, "Multicriteria distribution network reconfiguration considering subtransmission analysis," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2684–2691, 2010.

[59] I. Tristiu, M. Eremia, C. Bulac, and L. Toma, "Multi-criteria reconfiguration of distribution electrical networks for minimization of power losses and damage cost due to power supply interruption," in *Power Tech, 2007 IEEE Lausanne*. IEEE, 2007, pp. 385–390.

[60] F. Capitanescu, L. F. Ochoa, H. Margossian, and N. D. Hatziargyriou, "Assessing the potential of network reconfiguration to improve distributed generation hosting capacity in active distribution systems," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 346–356, 2015.

[61] R. Rao, K. Ravindra, K. Satish, and S. Narasimham, "Power loss minimization in distribution system using network reconfiguration in the presence of distributed generation," *IEEE transactions on power systems*, vol. 28, no. 1, pp. 317–325, 2013.

[62] L. Pfitscher, D. Bernardon, L. Canha, V. Montagner, V. Garcia, and A. Abaide, "Intelligent system for automatic reconfiguration of distribution network in real time," *Electric Power Systems Research*, vol. 97, pp. 84–92, 2013.

[63] R. Christie. Power systems test case archive. University of Washington, Electrical Engineering (UWEE). [Online]. Available: http://www.ee.washington.edu/research/pstca/

[64] M. Haraguchi and S. Kim, "Critical infrastructure systems: a case study of the interconnectedness of risks posed by hurricane sandy for new york city," *United Nation Office for Disaster Risk Reduction."Global Assessment Report on Disaster Risk Reduction." Accessed September*, vol. 8, p. 2016, 2014.

[65] *ISO 22301 - Business Continuity Management*, 2009.

[66] J. McLean, "Asset based approaches for health improvement: redressing the balance," *UK: Glasgow Centre for Population Health*, 2011.

[67] P. Alesi, "Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology," *Journal of Business Continuity & Emergency Planning*, vol. 2, no. 3, pp. 214–220, 2008.

[68] *CA Technologies - The Avoidable Cost of Downtime*, 2011.

[69] P. Woodman, V. Kumar *et al.*, "A decade of living dangerously: the business continuity management report 2009," 2009.

[70] *T. D. of ENISA Section Risk Management - Business and IT continuity overview and implementation principles*, 2008.

[71] B. Williamson, "Trends in business continuity planning: in business continuity planning, financial organizations are ahead of other types of businesses," *Bank Accounting & Finance*, vol. 20, no. 5, pp. 50–53, 2007.

[72] M. Arif, M. Katafygiotou, A. Mazroei, A. Kaushik, E. Elsarrag *et al.*, "Impact of indoor environmental quality on occupant well-being and comfort: A review of the literature," *International Journal of Sustainable Built Environment*, vol. 5, no. 1, pp. 1–11, 2016.

[73] J. Xing and E. Zio, "An integrated framework for business continuity management of critical infrastructures," in *ESREL 2016*, 2016.

[74] A. Giacchero, F. Giordano, and M. Schiraldi, "From business continuity to design of critical infrastructures: ensuring the proper resilience level to datacentres," *INTERNATIONAL JOURNAL OF ENGINEERING & TECHNOLOGY*, vol. 5, no. 4, pp. 3544–3553, 2013.

[75] *Telecommunications Industry Association (TIA), Telecomunications Infrastructure Standards for Data Centers - Rev.5.ANSI/EIA/TIA-942*, 2008.

[76] T. Drewitt, *A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system.* IT Governance Ltd, 2013.

[77] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for critical infrastructure protection. part i: A state of the art," *JRC Technical Notes*, 2012.

[78] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, "Critical infrastructure interdependency modeling: a survey of us and international research," *Idaho National Laboratory*, vol. 25, p. 27, 2006.

[79] J. López-Silva, V. A. Bañuls, and M. Turoff, "Scenario based approach for risks analysis in critical infrastructures." in *ISCRAM*, 2015.

[80] R. E. Walton, "A vision-led approach to management restructuring," *Organizational Dynamics*, vol. 14, no. 4, pp. 5–16, 1986.

[81] J. H. Jackson and C. P. Morgan, *Organization Theory.* Edition Prentice Hall Upper Saddle River, 1982.

[82] J. Xing and E. Zio, "An intj. xing, e. zioegrated framework for business continuity management of critical infrastructures." in *ESREL*, 2016.

[83] G. James. 9 reasons that open-space offices are insanely stupid. [Online]. Available: https://www.inc.com/geoffrey-james/why-your-company-will-benefit-from-getting-rid-of-open-office-spaces-first-90.html

[84] Y. Lv, G. Huang, L. Guo, Y. Li, C. Dai, X. Wang, and W. Sun, "A scenario-based modeling approach for emergency evacuation management and risk analysis under multiple uncertainties," *Journal of hazardous materials*, vol. 246, pp. 234–244, 2013.

[85] M. Branda, "Sample approximation technique for mixed-integer stochastic programming problems with several chance constraints." pp. Oper. Res. Lett. 40, 207–211, 2012.

[86] C. W. Y. C. Q. Tan, G.H. Huang, "If-em: an interval-parameter fuzzy linear programming model for environment-oriented evacuation planning under uncertainty." p. 286–303, 2011.

[87] X. Y. Y. C. Y. L. C.Z. Wu, G.H. Huang, "An interval-parameter mixed integer multi-objective programming for environment-oriented evacuation management," *Int. J. Syst. Sci.*, vol. 41, p. 547–560, 2010.

[88] "Integrating multi-agent evacuation simulation and multi-criteria evaluation for spatial allocation of urban emergency shelters." *International Journal of Geographical Information Science*, pp. 1–27, 2018.

[89] K. Mei, Yanlan; Xie, "Evacuation strategy of emergent event in metro station based on the electre method." pp. 1–10, 2018.

Publications & Deliverable

Journal papers

1. (2018) **Smart Behavioural Filter for Industrial Internet of Things**, Corbò, G., Foglietta, C., Palazzo, C. et al., Springer Mobile Network and Applications 2018 23: 809. DOI: 10.1007/s11036-017-0882-1. (Clarivate IF for 2017: 2.497).

2. (2017) **From Detecting Cyber-Attacks to Mitigating Risk Within a Hybrid Environment**, Foglietta, C., Masucci, D., Palazzo, C., Santini, R., Panzieri, S., Rosa, L., Cruz, T., and Lev, L., IEEE Systems Journal, 2018. DOI: 10.1109/JSYST.2018.2824252. (Clarivate IF for 2017: 4.337).

Books

1. (2018) **Chapter: Smart Buildings: Edifici Intelligenti per Migliorare l'Efficienza Energetica e il Comfort degli Utenti**, Smart Environments.

2. (2017) **Chapter: Intelligent Management for Smart Buildings (In-Press)**, ELSEVIER - Handbook of Energy Efficiency in Buildings.

Conference papers

1. (2018) **Evacuation Management Multi-Criteria Risk Assessment Based**, Masucci, D., Palazzo, C., Panzieri, S., ICBR - International Conference on Building Resilience, Lisbon, Portugal.

2. (2018) **Critical Infrastructure Risk Assessment Framework for Enterprise Business Continuity**, Palazzo, Cosimo & Orlando, Alessio & Panzieri, Stefano, IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Arlington, Virginia, USA.

3. (2018) **Smart Environment Monitoring Testbed**, D.Masucci, C.Foglietta, C.Palazzo, S.Panzieri, ICICT 2018, Cambridge city, UK.

4. (2017) **A Gateway-Centric IoT Framework for Open Hardware Platforms**, C.Palazzo, S.Panzieri, F.De Cillis, R.Setola., ICC 2017, Cambridge city, UK.

5. (2016) **Decision Support System for Electrical Grid Operators using a Multi-Criteria Algorithm with CISIApro Hybrid Risk Evaluation**, C.Palazzo, C.Foglietta, D.Masucci, S.Panzieri, SIDRA 2016, Rome, Italy.

6. (2016) **Smart Behavioural Filter for SCADA Network**, G.Corbò, C.Foglietta, C.Palazzo, S.Panzieri, INISCOM 2016, Leicester, UK.

7. (2016) **Improved Multi-Criteria Distribution Network Reconfiguration with Information Fusion**, C.Palazzo, C.Foglietta, D.Masucci, S.Panzieri, FUSION 2016, Heidelberg, Germany.

8. (2016) **Gestione delle Emergenze tramite Modelli di Interdipendenza nel Proggetto URANIUM**, C.Palazzo, C.Foglietta, D.Masucci, S.Panzieri, VGR 2016, Rome, Italiy.

9. (2016) **Enhancing Decision Support with Interdependency Modeling**, D.Masucci, C.Palazzo, C.Foglietta, S.Panzieri, In: Rice M., Shenoi S. (eds) Critical Infrastructure Protection X. ICCIP 2016. IFIP Advances in Information and Communication Technology, vol 485. Springer, Cham. Arlington, Virginia, USA.

10. (2016) **Managing Decisions for Smart Grid Using Interdependency Modeling**, Imbrogno, Simone & Foglietta, Chiara & Palazzo, Cosimo & Panzieri, Stefano, In proc. of 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (COGSIMA 2016), San Diego, CA, USA. DOI: 10.1109/COGSIMA.2016.7497810.

11. (2015) **Emergecy Management with Interdependency Modeling in the URANIUM Project**, Panzieri, Stefano & Palazzo, Cosimo & Masucci, Dario, In proc of TIEMS 2015. Rome, Italy.

12. (2015) **Assessing Cyber Risk Using the CISIApro Simulator**, Foglietta, Chiara & Palazzo, Cosimo & Santini, Riccardo & Panzieri, Stefano, In proc. of International Conference on Critical Infrastructure Protection, pp. 315-331. Arlington, Virginia, USA DOI: 10.1007/978-3-319-26567-4_19.

European Projects

- (2014) CIPS **FACIES** [online identification of Failure and Attack on interdependent Critical InfrastructurES]
- (2014) FP7 **CockpitCI** [Cyber-security on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures]
- (2015) CIPS **URANIUM** [Unified Risk Assessment Negotiation via Interoperability Using Multi-sensory data]
- (2016-2018) H2020 **ATENA** [Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures]
- (2018-today) H2020 **RESISTO** [RESilience enhancement and risk control platform for communication infraSTructure Operators]