

Antonio Di Pietro

METHODOLOGIES FOR EMERGENCY MANAGEMENT
IN CRITICAL INFRASTRUCTURES

Doctoral Thesis in
Computer Science and Automation
Dept. of Engineering
University of "Roma Tre"



University of "Roma Tre"

Doctoral Thesis in
Computer Science and Automation
Dept. of Engineering

XXVII Cycle

METHODOLOGIES FOR EMERGENCY MANAGEMENT
IN CRITICAL INFRASTRUCTURES

Ph. D. Student: Antonio Di Pietro Signature: _____

Advisor: Stefano Panzieri Signature: _____

Course Coordinator: Stefano Panzieri Signature: _____

April 2015

*Methodologies for Emergency Management
in Critical Infrastructures*

A Thesis presented by
Antonio Di Pietro
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Computer Science and Automation
Dept. of Engineering

University of "Roma Tre"

April 2015

I went to the woods because I wished to live deliberately, to front only the essential facts of life, and see if I could not learn what it had to teach, and not, when I came to die, discover that I had not lived.

— Henry David Thoreau

Dedicated to Laura, Francesco, Benedetta
and to the loving memory of my dad.

ABSTRACT

Critical Infrastructure Protection (CIP) is a concept that relates to the preparedness and response to severe incidents involving the critical infrastructures of a country. These incidents include terrorist attacks or large black-outs that may produce severe consequences for the citizens and the society in general.

Traditionally, each infrastructure takes care of its own system. For example, reliability indexes are used by the electrical utility to measure the quality of the electrical service. However, after the events of 9/11, Katrina, and others, it became clear that considering infrastructures separately was not sufficient to prepare for and respond to large disasters in an effective manner that prioritizes not the individual infrastructure states but the overall societal impact. A new era of research on interdependencies and best decisions during emergencies emerged.

A relatively large body of knowledge has built in recent years for modeling the CI interdependencies problem from a number of points of view. This is an area that affects society as a whole and, therefore, many disciplines have to come together for its understanding including computer science, systems engineering, and human aspects.

This thesis represents an extensive and thorough work not only in reviewing the state-of-the art in critical infrastructure protection but also in bringing together, within an integrated structural framework, a number of models that represent various aspects of the problem. This framework is applied to build and analyze realistic scenarios.

The body of the thesis can be divided into three aspects: I) Preliminary Notions (Chapters 2 and 3), II) Situation Awareness and Impact Analysis Methodologies (Chapters 4, 5, and 6), and III) Decision Support Systems (Chapter 7). This sequence builds the path from data collection to situational awareness, to best responses.

ACKNOWLEDGEMENTS

These years of research and this doctoral thesis would have not been possible without the help and support of some people. That's why I want to express my gratitude to some of them.

First and foremost, I extend my gratitude to my Ph.D supervisor, Professor Stefano Panzieri, for his guidance and support throughout this work.

My special thanks also go to Dr. Vittorio Rosato for giving me the opportunity to attend this Ph.D. and for its useful suggestions on how to improve this work.

I also thank Dr. Andrea Gasparri for his dedication and teachings and for stimulating me to do a quality work.

I also like to thank Professor Josè Martì for inviting me twice at the Department of Electrical and Computer Engineering at the University of British Columbia in Vancouver, Canada. My experience spent there in his research group was really stimulating and gave me the opportunity to address new research areas.

I would like to thank all the staff of the MCIP Lab of the Department of Engineering of the University of Roma Tre. My special thanks go to Dr. Chiara Foglietta for sharing this course of study and for its support during these years.

I would like to thank all my colleagues of UTMEA-CAL Lab of ENEA for the fruitful discussions I had with many of them that allowed me to complete this work.

Finally, I extend my utmost gratitude to Laura and my family for their encouragement, patience and love, which made this work a reality.

Antonio Di Pietro

*University of Roma Tre
April 2015*

CONTENTS

1	INTRODUCTION	1
1.1	Overview	1
1.2	Contributions	2
1.2.1	Algorithms for Distributed Data Fusion	3
1.2.2	Impact assessment of Cyber-Attacks and Natural Hazards	4
1.2.3	Decision Support	4
1.3	Organization of the Dissertation	4
I	PRELIMINARY NOTIONS	7
2	MULTI-SENSOR DATA FUSION	9
2.1	Data Fusion	9
2.2	Data Fusion Models	10
2.3	Approaches to Handling Uncertainty	11
2.3.1	Bayesian Probability Theory	12
2.3.2	Possibility Theory	12
2.3.3	Dempster-Shafer Theory	13
2.4	Notions of Dempster-Shafer Theory	13
2.4.1	Basic Notions	13
2.4.2	Evidence Combination	14
2.4.3	Evidence Discounting	15
2.4.4	Pignistic Probability	16
2.5	Data Fusion Architectures	16
2.6	Chapter Summary	17
3	MODELING AND SIMULATION OF INTERDEPENDENT SYSTEMS	19
3.1	Overview	19
3.2	Modeling and Simulation Approaches	20
3.2.1	Empirical Approaches	20
3.2.2	Agent Based Approaches	21
3.2.3	System Dynamics Based Approaches	21
3.2.4	Economic Theory Based Approaches	21
3.2.5	Network Based Approaches	22
3.2.6	Other Approaches	23
3.3	Network based tools	23
3.3.1	i2Sim	24
3.3.2	CISIA	26
3.4	Other approaches	27
3.4.1	WebSimP	27
3.5	Chapter Summary	29
II	SITUATION AWARENESS METHODOLOGIES	31
4	DISTRIBUTED DATA FUSION FOR SITUATION AWARENESS	33

4.1	Data Fusion Using Distributed Gossip Algorithm . . .	35
4.1.1	Data Fusion Algorithm	35
4.1.2	Convergence Criteria	37
4.1.3	Case Study	37
4.2	Data Fusion using Distributed Gossip Algorithm with Evidence Discounting	49
4.2.1	Data Fusion Algorithm	50
4.2.2	Simulation Results	55
4.3	Chapter Summary	58
5	IMPACT ASSESSMENT OF CYBER THREATS	61
5.1	Overview	62
5.2	Detailed Review of SCADA Security Testbeds	62
5.2.1	Reference Model	62
5.2.2	Comparing SCADA Security Testbeds	65
5.3	An i2Sim Based SCADA Security Testbed	66
5.3.1	Software Architecture	67
5.3.2	Case Study	69
5.4	A CISIA Based SCADA Security Testbed	73
5.4.1	Software Architecture	73
5.4.2	Case Study	76
5.5	Chapter Summary	78
6	IMPACT ASSESSMENT OF NATURAL HAZARDS	79
6.1	Overview	79
6.2	Decision Support System Architecture	80
6.2.1	Risk Analysis	80
6.2.2	Software Architecture	82
6.3	Impact Assessment in Electrical Distribution Grids . .	86
6.3.1	Short Time Scale Impact Assessment	86
6.3.2	Implementation	87
6.3.3	Case Study	89
6.4	Chapter Summary	91
7	RESOURCES ALLOCATION IN EMERGENCY SCENARIOS	93
7.1	Overview	93
7.2	Genetic Algorithms Based Approaches	94
7.2.1	Load Shedding Problem	94
7.2.2	Crewmen Optimization Problem	101
7.3	Ordinal Optimization Based Approach	105
7.3.1	Problem Overview	105
7.3.2	Case Study	108
7.4	Simulation Based Approach	109
7.4.1	Problem Overview	109
7.4.2	Case Study	110
7.5	Chapter Summary	116
	III EPILOGUE	119
8	CONCLUSIONS	121

IV APPENDIX	123
A PROOFS	125
A.1 Lemma 1 Proof	125
A.2 Lemma 2 Proof	126
BIBLIOGRAPHY	129

LIST OF FIGURES

Figure 1	Approaches covered grouped according to the capability of situation awareness and the use of sensor.	3
Figure 2	An example of a production cell.	25
Figure 3	Input-Output representation of a CISIA entity.	26
Figure 4	DR-NEP-WebSimP architecture.	28
Figure 5	Communication framework among the infrastructures in the considered scenario.	38
Figure 6	Communication framework among the infrastructures in the considered scenario.	39
Figure 7	Sample scenario.	41
Figure 8	An example of expected damage scenario ([44] and [69] modified).	45
Figure 9	Linear regression between the average disconnections rate and the quantity of rain precipitation.	46
Figure 10	Fragility curve for the segmented pipeline [49].	47
Figure 11	Sample scenario: resources exchanged among the infrastructures.	51
Figure 12	Sample scenario: dependency layer graph \mathcal{G} . Values l , m , h stand for low, medium and high degree of coupling respectively.	54
Figure 13	Main components of the reference model of the SCADA security testbed.	62
Figure 14	Enhanced SIEM platform architecture.	67
Figure 15	Sample scenario.	70
Figure 16	MHR model of the example scenario.	71
Figure 17	OSSIM rule.	72
Figure 18	i2Sim results.	73
Figure 19	Reference architecture.	74
Figure 20	Main components and connections of Integrated Risk Predictor system.	75
Figure 21	Data workflow for a simple attack scenario.	76
Figure 22	Interdependences model in the MHR approach.	78
Figure 23	Functional Block Diagram of the Decision Support System.	83

Figure 24 Examples of Physical Harms Scenarios. Upper side: Shake map of a seismic event; Lower side: Flood risk. Each physical component is associated an estimated damage level resulting from the occurrence of the natural hazard (seismic and flooding event respectively). 85

Figure 25 The electrical distribution grid model. 87

Figure 26 Representation of a section of a power distribution grid of Rome. Rome scenario at time $t = t_0$ 89

Figure 27 Representation of a section of a power distribution grid of Rome. Rome scenario at time $t = t_2$ (hypothesis: BTS are working properly). 90

Figure 28 Profile of the estimated substations in failure state. 91

Figure 29 Sample scenario: functional dependencies involving a power grid, water distribution networks, hospitals and manufacturing plants. . . 96

Figure 30 Sample scenario: geographic representation the shake map relative to the seismic event. The lightning indicates the physical components that are estimated to be damaged due to the occurrence of the seismic event. 97

Figure 31 Power grid model. Grey boxes: power generators; red boxes: High Voltage substations; yellow boxes: Medium Voltage substations; arrow: electrical loads. 98

Figure 32 Case study: representation of a section of the electrical distribution grid of Rome. Arrows indicate the interdependency among Electrical and SCADA systems. 103

Figure 33 Case study: a candidate sequence solution for the optimization problem and a representation of the sequences of manual interventions over time. 104

Figure 34 Ordinal Optimization solution space [47]. . . . 107

Figure 35 Curves trend of the Physical Modes of the izsim model. 108

Figure 36 Hospital simulation results. 108

Figure 37 Power distribution grid and SCADA system. . . 111

Figure 38 SCADA System. 112

Figure 39 izsim Model. 113

- Figure 40 Steady-state convergence at different time-intervals.
The number inside each circle represents the
weight function set value $w_i(t_i, \gamma_a)$ of a generic
set $\gamma_a \in 2^\Omega \setminus \Omega$, associated to agent i 126

LIST OF TABLES

Table 1	An example of application of the cautious combination rule.	15
Table 2	An example of BBA $m(\cdot)$ and its relative discounting function $m^\alpha(\cdot)$ obtained for $\alpha = 0.2$	15
Table 3	Monitoring agents considered in the scenario.	42
Table 4	BBA generated by agent v_1	43
Table 5	BBA generated by agent v_2	43
Table 6	BBA generated by agents v_3 and v_5	44
Table 7	BBA generated by agent v_4	45
Table 8	BBA generated by agent 6 (P denotes PGA).	47
Table 9	An example of initial BBAs for agents v_i with $i = 1..11$ at time $t = 0$ and convergent BBA at time $\bar{t} = 106$	48
Table 10	BBA $m_i^f(0)$ applied to node v_i in case of link failure of e_{ij}	53
Table 11	Simulation results obtained with a static topology and time-unvarying confidences with convergent BBAs reached at time $\bar{t} = 5$	56
Table 12	Simulation results obtained with a static topology and time-varying confidences with convergent BBAs reached at time $\bar{t} = 43$	56
Table 13	Simulation results obtained with a dynamic topology and time-unvarying confidences with convergent BBAs reached at time $\bar{t} = 31$	57
Table 14	Simulation results obtained with a dynamic topology and time-varying confidences with convergent BBAs reached at time $\bar{t} = 50$	58
Table 15	Capabilities required for each of the identified categories.	65
Table 16	Electric demands of the CIs considered in the scenario.	70
Table 17	Electrical Power balance (active power, MW) resulting from the load shedding actions in case I and II.	97
Table 18	Critical Infrastructure Service Layer (Case I and II).	98
Table 19	Considered Consequence Criteria.	102
Table 20	Electricity demand for loads/customers.	111
Table 21	SCADA network model assumptions.	112
Table 22	Sequence of events for the simulated scenarios.	113
Table 23	Feasible configurations for 100% power supply to the water pumping station.	114

Table 24	Decision space for the three scenarios.	115
Table 25	Simulation results.	116

INTRODUCTION

1.1 OVERVIEW

Critical infrastructure are the assets, systems, and networks, whether physical or virtual that are essential for the functioning of a society and economy. Typical examples of critical infrastructures are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, and oil/natural gas pipelines.

The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may produce a significant negative impact for the security and the well-being of its citizens. In particular, the existence of dependencies of various type (e.g., physical or cyber) with different degree of coupling [60] [73] among the infrastructures expose them the possibility of cascading failures not only within the facility or the company, but also cascading effects that might affect other infrastructures [89].

For example, a black-out occurring in an electrical distribution network can produce disruptions for the telecommunication services which in turn may alter the normal functioning of banking services in a specific area thus causing negative effects for the citizens.

The protection of critical infrastructures is relevant in all industrialized countries. To this regard, specific policies have been produced to increase their security. In 2008, in the context of the European Programme for Critical Infrastructure Protection (EPCIP), a specific directive [33] establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection.

The literature on critical infrastructure protection is mostly provided by states that publish their national strategies to address the

challenge of protecting their critical infrastructures. The investigations of researchers have encompassed issues of national security, policymaking, infrastructure system organization, and behavior analysis and modeling.

Regarding the latter subject, in order to evaluate the risk of degradation of critical infrastructure services which may result in cascading failures, an improved *situation awareness*, aiming at identifying the state of a system and predict its evolution, can be of help for decision makers to take appropriate countermeasures.

Situation awareness [71] is formally defined as "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future*". When applied to critical infrastructures contexts, situation awareness encompass approaches at different hierarchical level according to the capability of providing high-level support to decision makers and the use of raw data coming from sensors. Hence, situation awareness is highly connected to the data fusion concept, where multiple information sources have to be combined, in order to provide a robust and complete description of an environment or process of interest [56].

In the field of physical security such as field surveillance, data fusion techniques are typically based on a huge availability of sensorial data used, for instance, to determine the presence of entities in the patrolled area (e.g., ships, submarines, air-crafts, etc.), with the aim of identifying them on the base of specific properties.

Hence, it is fundamental to provide adequate raw data aggregation methodologies, in order to obtain high-level behaviour detection and prediction to implement mitigating risks procedures addressing prevention, protection, preparedness, and consequence management.

1.2 CONTRIBUTIONS

In order to present the topics addressed in this dissertation, in Figure [Figure 1](#) we show the different contributions ordered by the grade of situation awareness provided by each of them and the relative use of sensors which they require.

As mentioned, data fusion make high use of raw data coming from several sources to produce new raw data so that fused data is more informative and synthetic than the original inputs. To this regard, we defined specific algorithms and proposed how the fused data produced by such algorithms may be used to increase the security of critical infrastructures. However, the algorithms proposed cannot be regarded as a means to provide an high situation awareness as they provide a raw estimation in a limited temporal horizon and make little use of past data.

Approaches for impact assessment have been proposed to predict the impact of specific cyber threats and natural hazards to critical in-

frastructures. Such approaches can model the relationships between functional components of critical infrastructures and the provided services to perform risk assessment and predict service level variations. Although they are based on data provided by sensors to detect cyber and natural threats, the focus of such approaches is to integrate raw data inside models that can estimate the service evolution in terms of expected damages or service losses and the effect of specific actions on the actors and entities involved.

Procedures to mitigate the risk of service degradations in critical infrastructures have been proposed in contexts where the resources, that are vital to ensure normal service levels, are limited. Such approaches can provide high situation awareness to decision makers and estimate the impact of decisions.

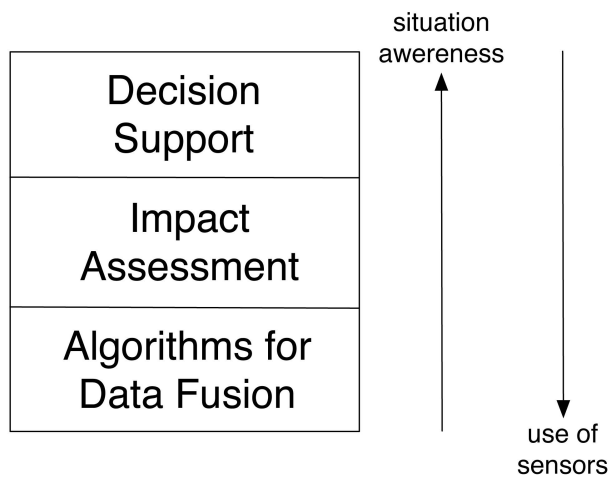


Figure 1: Approaches covered grouped according to the capability of situation awareness and the use of sensor.

1.2.1 *Algorithms for Distributed Data Fusion*

We propose a distributed communication framework to be implemented among dependent critical infrastructures based on information sharing of possible adverse events (e.g., physical, cyber) that affect the infrastructures.

The proposed framework, based on distributed data fusion algorithms, allows to produce early warnings against possible events that may cause cascading failures. This information can be useful for decision makers to take appropriate countermeasures.

For one of the two algorithms, we demonstrate the convergence in case of temporary failures affecting the communication channels that allow the sharing of the adverse events.

1.2.2 *Impact assessment of Cyber-Attacks and Natural Hazards*

We present a methodology to analyze realistic scenarios of cyber attacks and natural hazards and measure their consequences in terms of the impact on multiple interdependent infrastructures. This is a new key concept in the electric power grid at the present time, when the traditional "confined" grid is being "opened-up" to allow for distributed energy resources to be supplied by independent providers. The traditional concept of "reliability" of individual components in the grid is shifting towards the concept of "resiliency" of the grid, thus recognizing that the focus should be the ultimate impact on society.

Regarding the assessment of cyber attacks, we present two platforms and show how threats against wireless sensor network nodes and SCADA components can be detected to conduct real-time assessments of the impact of the attacks on the services provided by critical infrastructures.

Regarding the assessment of natural hazards, we describe the main features of a Decision Support System (DSS) employing modeling and simulation techniques to forecast the effects of natural hazards. Then, we present a predefined procedure that produces an estimate of the number of electrical substations of an electric distribution grid by considering the interdependency phenomena with the relative SCADA system.

1.2.3 *Decision Support*

We present methodologies that can be valuable for decision makers to define optimal allocation of resources that maximize the delivery of infrastructure services during emergency crisis.

The actions proposed to decision makers are produced by keeping into account the interdependency existing among the power domain and the SCADA system so that the consequences for the society may be reduced.

1.3 ORGANIZATION OF THE DISSERTATION

The rest of the dissertation is organized into two main parts and an epilogue dedicated to the future research directions and concluding remarks.

Part I: Preliminary Notions contains introductory material that is essential to understanding the rest of the dissertation.

Chapter 2 provides a brief introduction to data fusion with a special focus to Dempster-Shafer formalism relevant to the work presented in this dissertation.

Chapter 3 presents a review on modeling and simulation of interdependent critical infrastructures methodologies. In particular, we describe the methodologies and tools used to implement impact assessment and procedures for emergency management.

Part II: Situation awareness methodologies contains approaches analysed to implement situation awareness.

Chapter 4 presents two data fusion frameworks based on distributed gossip algorithms to exchange the possible cause(s) of fault or threat affecting critical infrastructures to increase their security security. We also present practical methods that can be implemented by sensor points installed at each infrastructure to estimate specific threats.

Chapter 5 studies the problem of how to estimate the impact of cyber threats affecting critical infrastructures. We first present a taxonomy of SCADA security testbeds taken from the literature which allow to recreate cyber-attacks on the de facto standard communication protocol. Then, we present specific technological frameworks able to assess the impact of cyber threats against specific nodes of SCADA systems controlling interdependent physical systems.

Chapter 6 studies the problem of how to estimate the impact of natural hazards affecting critical infrastructures. We present the functionalities of a Decision Support System (DSS) and show an application of the system to a sample crisis scenario induced by an earthquake. We then present a procedure to assess the impact of natural hazards in electric and SCADA systems.

Chapter 7 provides methodologies based on optimization techniques to implement mitigation strategies.

Part III: Epilogue contains the concluding chapters of the dissertation.

Chapter 8 provides concluding remarks and presents future research directions to extend the proposed work.

Part I

PRELIMINARY NOTIONS

Multi-sensor data fusion techniques provide refined information from multiple sensor data sources by spatio-temporal data integration and the available context.

In the context of public security, it is of outstanding importance to aggregate raw data obtained from multiple sources in order to provide an improved picture of a situation as well as to gather knowledge about all the actors in a scenario. In tactical operations, either in the military or for civil purposes, data fusion is a process that increases intelligence tasks and provides important support for planning operations.

This Chapter is organized as follows: in Section 2.1 we present an overview on data fusion; in Section 2.2 we discuss the popular data fusion models; in Section 2.3 we describe the main formalisms to handle uncertainty in data fusion contexts; in Section 2.4 we focus on the Dempster-Shafer data fusion formalism, and finally in Section 2.5 we discuss the different data fusion architectures.

2.1 DATA FUSION

In general, the terms information fusion and data fusion are used as synonyms even if in some cases the term data fusion is used for raw data i.e., data obtained directly from the sensors whereas the term information fusion is employed when considering already processed data. In the literature, there are different terms related to data fusion which include decision fusion, data combination, data aggregation, multi-sensor data fusion, and sensor fusion.

White [92] defines data fusion as "a process dealing with the association, correlation, and combination of data and information from single and multiple sources to achieve refined position and identity estimates, and complete and timely assessments of situations and threats,

and their significance. The process is characterized by continuous refinements of its estimates and assessments, and the evaluation of the need for additional sources, or modification of the process itself, to achieve improved results".

Briefly, we can define multi-sensor data fusion as the process through which data are combined from multiple sources whereas single-sensor fusion refers to the case where multiple data coming from a single source are fused. In both cases, data aggregation is performed to obtain improved information i.e., information that has higher quality or more relevant information content.

Data fusion techniques can be grouped into three categories: (i) data association, (ii) state estimation, and (iii) decision fusion [17].

Data association techniques try to establish the set of measurements that are generated by the same target over time (e.g., a track can be defined as a sequence of points along a path provided by the same target). Data association is often executed before the state estimation of the detected targets. Data association process can be performed in all of the fusion levels with a granularity that depends on the specific level.

State estimation techniques allow to estimate the state of the target under movement given a set of measurements. Target observations may or may not be relevant, which means that in general only some of the observations could actually be associated to the target. State estimation methods include linear and nonlinear dynamics and measurements. In first case, the equations of the object state and the measurements are linear and the noise follows the Gaussian distribution; theoretical solution are based on the Kalman filter. In nonlinear dynamics, the state estimation problem there are methods based on control theory and probability to define a vector state from vector measurements.

Decision fusion techniques produce a high-level inference about the events and activities that are generated from the detected targets. These techniques can be based on Bayesian methods, Dempster-Shafer inference, adductive reasoning or semantic methods.

2.2 DATA FUSION MODELS

Endsley [34] proposed a data fusion model known as Joint Directors of Laboratories (JDL) based on four-layered hierarchical structure where each layer provides a descriptive representation of the scenario. In this model, moving from the lower to the higher layer, the degree of information is decreased whereas the degree of information is increased due to the data aggregations implemented at each layer.

Level 1 Object Refinement: This layer attempts to identify objects and entities involved in the scenario by fusing the properties of

the objects from multiple sources. Data gathered at this stage provide a low degree of abstraction (e.g., position, speed).

Level 2 Situation Assessment: This layer attempts to evaluate the relations among the different entities and the observed events provided by level 1.

Level 3 Threat Assessment: This layer predicts the effect of the situation identified by level 2 in terms of possible opportunities for operation (e.g., expected damages given the enemy's behaviour).

Level 4 Process Refinement: This layer allocates sources to mission goals and highlights the impact of these decisions.

Thomopoulos [84] proposed a model for data fusion consisting of three modules, each integrating data at different levels namely Signal, Evidence and Dynamics level fusion. Signal level fusion applies data correlation through learning due to the lack of a mathematical model describing the phenomenon being measured. Evidence level fusion combines the data at different levels of inference based on a statistical model and the assessment required by the user. Dynamics level fusion applies the fusion of data through the support of specific mathematical models.

The presented two models should not be considered as operative procedures, but rather methodologies that may be useful to adequately define the steps for the extrapolation of high-level and abstract information from raw low-level data.

2.3 APPROACHES TO HANDLING UNCERTAINTY

Mechanisms to handle uncertain data is required in every data fusion framework. Uncertain data result from lack of information in a specific area of interest. The types of uncertainty can be grouped as follows [23]:

Incompleteness: relates to the situation where part of the information required is missing (e.g., if the position of the detected hostile unit is missing from a report then the report information is incomplete).

Imprecision: relates to the situation where the value of a variable of interest is given but not with enough information (e.g., the temperature value detected by a thermometer is between 15 and 25 Celsius degrees).

Uncertainty: relates to the situation where the information is complete, precise but uncertain since it may be wrong (e.g., the tem-

perature value detected by a thermometer is probably 25 Celsius degrees).

Depending on the mechanism used to handle uncertainty, the kinds of uncertainty that can be treated for data representation, fusion, inferring and decision-making by a specific approach may vary.

In the following, we present a brief introduction of the popular methodologies to handle uncertainty in order to show each approach can accommodate specific properties of uncertain data.

2.3.1 *Bayesian Probability Theory*

The Bayesian Probability Theory provides an interpretation of the concept of probability. This can be seen as an extension of propositional logic that enables reasoning with hypotheses, i.e., the propositions which deal with uncertainty.

In contrast to interpreting probability as the frequency of some phenomenon, Bayesian probability is a quantity that denotes a state of belief or knowledge. Beliefs are always subjective, and therefore all the probabilities in the Bayesian Probability Theory are conditional to the prior assumptions and experience of the learning system. Some disadvantages of this Bayesian Probability Theory are the difficulty in defining prior likelihoods when information is not available and the fact that the hypotheses must be mutually exclusively.

2.3.2 *Possibility Theory*

Possibility theory was introduced by Zadeh [94] as an extension of his theory of fuzzy sets and fuzzy logic. It differs from classical probability theory by the use of a pair of dual set-functions i.e., possibility and necessity measures instead of only one. A possibility measure is a set function that returns the maximum of a possibility distribution over a subset indicating an event. A necessity measure is a set function associated to a possibility measure through a relation expressing that an event is more certain than another one. This feature makes it easier to capture partial ignorance.

Where the vagueness of information needs to be modeled, approaches based on possibility theory are more suitable than those based on probability theory. The high number of computations required by this approach w.r.t. other ones and the complexity in generating appropriate membership functions are the main disadvantages of this technique.

2.3.3 Dempster-Shafer Theory

This theory, introduced by Dempster [27] and Shafer [79] also known as Dempster-Shafer Theory (DST), embraces the intuitive idea of associating a number between zero and one to model the degree of confidence for a proposition from partial (uncertain, imprecise) evidence.

DST has become one of the most used frameworks for handling uncertainty in various fields of applications. One of the major advantages of DST over probability theory is to allow one to specify a degree of ignorance in a situation instead of being forced to supply prior probabilities. Respect to probabilistic approaches that can reason only on singletons, DST allows not only to affect belief on elementary hypotheses but also on composite ones. The latter illustrates the fact that DST manages also imprecision and inaccuracies.

Based on these facts, the decision-making capabilities implemented with DST are much more flexible than the probability theory. One disadvantage of this methodology is given by the exponentially large computation overhead that is required to implement the additional modeling flexibility.

2.4 NOTIONS OF DEMPSTER-SHAFER THEORY

In this Section, we introduce some concepts of DST that are relevant for the data fusion contributions presented in Chapter 4.

2.4.1 Basic Notions

In the DST, the set propositions that a node can evaluate is called Frame of Discernment (FoD) $\Omega = \{\omega_1, \dots, \omega_n\}$ where the elements ω_i are assumed to be mutually exclusive.

Let $\Gamma(\Omega) \triangleq 2^\Omega = \{\gamma_1, \dots, \gamma_{|\Gamma|}\}$ be the power set associated to it. In this framework, the interest is focused on quantifying the confidence of propositions of the form: "The true value of ω is in γ ," with $\gamma \in 2^\Omega$.

Definition 1 (Basic definitions). *A function $m : 2^\Omega \rightarrow [0, 1]$ is called a basic belief assignment (BBA) m if $\sum_{\gamma_a \in 2^\Omega} m(\gamma_a) = 1$ with $m(\emptyset) = 0$. A BBA m can equivalently be represented by its associated commonality $q : 2^\Omega \rightarrow [0, 1]$ defined as:*

$$q(\gamma_a) = \sum_{\gamma_b \supseteq \gamma_a} m(\gamma_b), \quad \gamma_a \in 2^\Omega \quad (1)$$

Thus, for $\gamma_a \in 2^\Omega$, $m(\gamma_a)$ is the part of confidence that supports exactly γ_a i.e., the fact that the true value of ω is in γ_a but, due to the lack of further information, does not support any strict subset of γ_a .

2.4.2 Evidence Combination

The limitation of the DST formulation regards the application of the Dempster combination rule [79], that produces counterintuitive results whenever there is a strong conflict among the sources to be combined [93]. A different approach is based on the Transferable Belief Model (TBM) defined by Smets [80], which relies on the concept of BBA but removes the assumption of $m(\emptyset) = 0$. The removal of this assumption applies when the frame of reference is not exhaustive, so that it is reasonable to believe that another event, not modeled in the considered frame, will occur. This allows to define a more refined rule, the TBM conjunctive rule [28], that is more robust than the Dempster combination rule, in the presence of conflicting evidence.

Definition 2 (TBM conjunctive rule \otimes). *In the TBM, the combination rule removes the normalization constant in the Dempster combination rule and therefore is defined as follows:*

$$m_{ij}(\gamma_a) = \sum_{\gamma_b, \gamma_c: \gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c), \quad \gamma_a \in 2^\Omega \quad (2)$$

The TBM conjunctive rule is associative and its use is appropriate when the conflict is related to poor reliability of some of the sources. However, such a rule, together with the Dempster combination rule, relies on the distinctness assumption of the sources or, in other words, that the information sources be independent. This limitation can be avoided using a combination rule that observes the idempotence property. Denoeux [29] defines an associative, commutative and idempotent operator, called cautious rule of combination, that is appropriate when all sources are considered reliable and does not require the assumption of independence.

Definition 3 (weight function). *Let m be a generic BBA, the weight function $w : 2^\Omega \setminus \Omega \rightarrow \mathbb{R}^+$ is defined as:*

$$w(\gamma_a) = \prod_{\gamma_b \supseteq \gamma_a} q(\gamma_b)^{(-1)^{|\gamma_b| - |\gamma_a| + 1}}, \quad \forall \gamma_a \in 2^\Omega \setminus \Omega \quad (3)$$

$$= \begin{cases} \frac{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \notin 2\mathbb{N}} q(\gamma_b)}{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \in 2\mathbb{N}} q(\gamma_b)}, & \text{if } |\gamma_a| \in 2\mathbb{N}, \\ \frac{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \in 2\mathbb{N}} q(\gamma_b)}{\prod_{\gamma_b \supseteq \gamma_a, |\gamma_b| \notin 2\mathbb{N}} q(\gamma_b)}, & \text{otherwise,} \end{cases}$$

Definition 4 (Cautious rule of combination \odot). *Let m_i and m_j be two generic BBAs in the TBM with weight functions w_i and w_j respectively. Their combination using the cautious conjunctive rule is noted $w_i \odot_j = w_i \odot w_j$. It is defined as the following weight function:*

$$w_{i \odot_j}(\gamma_a) = w_i(\gamma_a) \odot w_j(\gamma_a) = \min(w_i(\gamma_a), w_j(\gamma_a)), \quad \forall \gamma_a \in 2^\Omega \setminus \Omega \quad (4)$$

Table 1: An example of application of the cautious combination rule.

BBA	\emptyset	a	b	Ω
$w_1(\cdot)$	1	0.5	0.3	
$w_2(\cdot)$	0.8	0.7	0.2	
$w_{1\otimes 2}(\cdot)$	0.8	0.5	0.2	

 Table 2: An example of BBA $m(\cdot)$ and its relative discounting function $m^\alpha(\cdot)$ obtained for $\alpha = 0.2$.

BBA	\emptyset	a	b	Ω
$m(\cdot)$	-	0.3	0.4	0.3
$w(\cdot)$	1.4	0.5	0.4	
$m^{0.2}(\cdot)$	-	0.06	0.08	0.86
$w^{0.2}(\cdot)$	1	0.93	0.91	

The data aggregation algorithms presented in Chapter 4 work with the weight function $w(\cdot)$, which is obtained from masses using commonality function $q(\cdot)$, derived from the initial set of BBAs.

Table 1 shows the function $w_{1\otimes 2}(\cdot)$ obtained by applying the cautious combination rule among two weight functions w_1 and w_2 . From now on, we denote with $w_{ij}(\cdot)$ the weight function obtained from the application of the cautious combination rule among two generic weight functions $w_i(\cdot)$ and $w_j(\cdot)$.

2.4.3 Evidence Discounting

The evidence discounting concept was introduced by Shafer [79] for accounting the reliability of a source information. Other works by Cherfaoui et al. [19, 20] applied the evidence discounting in a network of agents according to the distance and the age of the received message before to combine it with a local knowledge.

Definition 5 (Discounting function). *Let m be a generic BBA. The relative discounting function $m^\alpha(\gamma_a)$ can be defined as follows:*

$$m^\alpha(\gamma_a) = \begin{cases} \alpha m(\gamma_a), & \text{for } \gamma_a \subset \Omega, \\ 1 - \alpha + \alpha m(\gamma_a). & \text{for } \gamma_a = \Omega. \end{cases}$$

where $\alpha \in [0, 1]$ is called the discounting factor.

Table 2 shows an example of BBA $m(\cdot)$ and its relative discounting function $m^\alpha(\cdot)$ obtained for $\alpha = 0.2$. The table also reports the weight functions associated to the two BBAs.

When the reliability α of an information source is known, it can be used to discount evidence before executing fusion operations.

2.4.4 Pignistic Probability

Pignistic probability [80], in decision theory, is a probability that can be assigned to an option in order to make a decision although there might be lack of knowledge or uncertainty about the options and their actual likelihoods.

As it will be clear in Chapter 4, we use pignistic probability to provide an indication of the results obtained by our data aggregation algorithms. In particular, we use the pignistic transformation to transform a BBA $m(\cdot)$ into a probability measure $P_m = \text{Bet}(m)$ as follows:

$$P_m(\gamma_a) = \sum_{\emptyset \neq \gamma_b \subseteq \Omega} m(\gamma_b) \frac{|\gamma_a \cap \gamma_b|}{|\gamma_b|}, \quad \gamma_a \in 2^\Omega \quad (5)$$

2.5 DATA FUSION ARCHITECTURES

Depending on the architecture type, data fusion techniques can be classified as: (i) centralized, (ii) distributed, and (iii) decentralized [17].

In a centralized architecture, the fusion node is placed in the central processor that acquires the information from all of the input sources. Hence, the fusion processes are implemented in a central processor that uses the provided raw measurements from the different sources.

In a distributed architecture, measurements from each source node are processed independently before the information is sent to the fusion node, which receives information from all the nodes. This type of architecture provides different variations that range from only one fusion node to several intermediate fusion nodes. Distributed algorithms usually share their state (e.g., position, velocity) with the associated probabilities to perform the fusion process.

In a decentralized architecture, each node combines its local information with the information that is received from its peers to reach a common knowledge about an event of interest. Considering that the decentralized data fusion algorithms exchange information instead of states and probabilities, they have the advantage of easily separating old knowledge from new knowledge.

In the ideal case, the decentralized common knowledge should converge to the centralized solution, which is considered to be optimal. In general, this can be easily achieved when the states are static. However, for dynamic states, additional constraints are required.

In Chapter 4 we present a decentralized data fusion algorithm and show results proving the convergence of the algorithm.

2.6 CHAPTER SUMMARY

In this Chapter, we gave an presented the data fusion problem and discussed the methodologies used to handle uncertain information in data fusion frameworks.

Then, we presented key notions of Dempster-Shafer Theory and motivated why this approach is suitable for handling uncertain data w.r.t. other methodologies.

Finally, we presented different data fusion architectures and presented the main advantages of decentralized approaches w.r.t. distributed approaches.

Modeling and simulation of interdependencies of critical infrastructures has become a considerable field of research with the aim to improve infrastructure support planning, maintenance and emergency decision making. Ouyang [64] reviewed all the research in this field by grouping the existing modeling and simulation approaches into six branches: (i) empirical; (ii) agent based; (iii) system dynamics based; (iv) economic based (v) network based, and (vi) other approaches.

In this Chapter, we recall the main principles and applications of the mentioned approaches and focus on two network based approaches that have been used as tools for impact assessment presented in Chapters 5 and 6. We also present an approach based on a distributed simulation platform that was adopted to implement emergency resources allocation problems presented in Chapter 7.

3.1 OVERVIEW

Interdependencies increase the vulnerability of the corresponding infrastructures as they the propagation of failures from one infrastructure to another with the consequence that the impact due to failures of infrastructure components and their severity can be exacerbated compared to failures confined to single infrastructures.

There different definitions of infrastructure interdependencies. Rinaldi et al. [74] grouped them according to six dimensions:

- the type of interdependencies e.g., physical, cyber, and logical;
- the infrastructure environment e.g., technical, business, political, legal;
- the couplings among the infrastructures and their effects on their response behavior (loose or tight, inflexible or adaptive);

- the infrastructure characteristics: organizational, operational, temporal, spatial;
- the state of operation (normal, stressed, emergency, repair), the degree to which the infrastructures are coupled;
- the type of failure affecting the infrastructures: common-cause (when two or more infrastructures are affected simultaneously because of some common cause), cascading (when a failure in one infrastructure causes the failure of one or more component(s) in a second infrastructure), and escalating (when an existing failure in one infrastructure exacerbates an independent failure in another infrastructure).

The latter definitions together with governmental reports containing recommendations and policies for the protection of critical infrastructures, can be considered as conceptual and qualitative based approaches. In fact, both provide the definitions of infrastructures and their interdependencies and highlight the importance to protect critical infrastructures by proposing specific strategies to reach this objective.

However, these approaches do not provide any detailed modeling and simulation approach to analyze infrastructures behavior.

3.2 MODELING AND SIMULATION APPROACHES

3.2.1 *Empirical Approaches*

Empirical approaches consider infrastructure interdependencies based on historical disruptions data and expert experience. Contributions in this area try to identify frequent and significant failure patterns, model interdependency strength metrics and propose approaches based on risk analysis.

In order to identify frequent and significant failure patterns, special databases have been created from incidents reports such as the earthquake in Japan and the hurricanes in Florida and some others. These data are usually extracted from media reports and official documents issued by infrastructure operators and can be used to define metrics to assess the consequences of a failure under extreme events. For example, McDaniels et al. [57] defined two indexes: (i) an impact index given by the product of the failure duration and severity weights; and (ii) an extent index given by the product of the failure spatial extent and the number of people involved.

Zimmerman et al. [97] introduced several interdependency related indicators to have information about: (i) the infrastructure components that frequently produce an impact for other infrastructures; (ii) the ratio of being a cause of failure to being impacted by failures and (iii) the number of people affected by a failure.

Utne et al. [88] designed a cascade diagram showing how an initiating event can be propagated across different infrastructures. Based on historical failure data and the knowledge of past incidents, they were able to assess the frequency of the initiating event, the probabilities of all involved events, the number of people being affected, and the duration of the subsequent events.

3.2.2 Agent Based Approaches

Agent based approaches adopt a bottom-up view and consider the overall behavior of the system of interconnected infrastructures emerging from a plethora of interacting agents where each agent models one or more physical infrastructure components or services.

Aspen [13] is an agent based model used to model the economic consequences of decisions and was used to assess the outcome of federal monetary policies. RePast [22] is an agent framework for the development of agent models allowing creation and execution of simulations. RePast contains libraries for implementing genetic algorithms and neural networks to design agents business rules. NetLogo [86] is a multi-agent programming language addressing natural and social sciences phenomena where each agent allows to discover of emergent behaviors.

3.2.3 System Dynamics Based Approaches

System Dynamics (SD) based approaches adopt a top-down view to study interdependent systems. In this kind of approaches, there exist constructs that can be used inside each model to represent specific behavior and objects. In particular, *feedback loops* allow to model an effect between infrastructure components or services (e.g., the electrical power provided by a system feeding an hospital) whereas *stocks* can be used to model the level of a specific resource (e.g., the quantity of water in a tank). SD based approaches can model dynamic (i.e., inertial) states through the use of differential equations to describe the system level behaviors of the infrastructures.

CIP/DSS [78] is a Decision Support System based on SD that was used to model the interdependencies existing among water, public health, emergency systems, telecom, energy and transportation infrastructures. Its application allows to estimate the effect of possible disruptions occurring in such systems and to evaluate the effect of mitigations actions.

3.2.4 Economic Theory Based Approaches

Economic theory based approaches fall in two main areas: Input-Output (I-O) and Computable General Equilibrium (CGE) models.

I-O models [52] were defined by Leontief to represent the technological relationships of productions. Leontief proposed a linear model where the total production output of each industry sector is related to the production of other sectors according to specific weights. The resulting system provides a unique solution so that a final demand vector can be found. Based on the Leontief I-O model, Haines and Jiang proposed the Input-Output Inoperability (IIM) [45] model where they consider the output of the Leontief model as the inability or *inoperability* of an infrastructure to perform specific services. Given a perturbation from one or more infrastructures or industries of the economy, the model can assess the consequences in terms of infrastructures or industry inoperability.

Computable General Equilibrium (CGE) can be considered as an extension of the I-O models. Based on actual economic data, they can estimate how an economy might react to changes in policy, technology or other external factors. Rose and Liao [75] developed a CGE model to study the economic resilience of the city of Portland to an earthquake that produces disruptions on the water supply network. The model allowed to evaluate the effectiveness of resilience improvements actions such as prevent water pipeline replacement. A similar approach was used by Rose et al. [10] to analyze the economic effects of a terrorist attack against the Los Angeles power grid. The economic estimate produced by the CGE based model demonstrated the benefit of mitigation actions aiming at improving the power grid such as onsite electricity generation and rescheduling of production.

3.2.5 Network Based Approaches

Network based approaches model infrastructure interdependencies by representing each infrastructure through its network topology where nodes mimic physical components and the relations among them. There exist two main approaches: (i) *topology based methods* where each network node exhibit two states (normal and failed) depending if the work properly or they affected by the occurrence of hazards or due to intra- or interdependencies phenomena and (ii) *flow based methods* that take focus on the services provided and distributed among the infrastructures.

Topology based methods allow to define various metrics to evaluate the performance response of the infrastructures under different hazards. For instance, the performance of each network can be assessed by the connectivity loss, the number of normal or failed physical components, the duration of components unavailability, the number of customers served or affected [31, 67]. By quantifying the interdependent effect, performance metrics can facilitate the assessment of mitigation actions such as adding bypass or hardening specific components performance. In this regard, specific strategies can

be compared by considering the response of networks with different topological structures in terms of component degree, component betweenness etc.

In Flow based methods, nodes and edges are entities able to produce and distribute the services. Following this approach, Lee et al. [51] proposed a model where each node includes a supply or a demand node or a transshipment node and each arc has a predefined capacity. It allows to mathematically define the interdependencies relations and to and evaluate specific restoration plans. Such a model was used to evaluate the operations of health care facilities in crisis scenarios. Rosato et al. [77] modeled an electrical network through Direct Current (DC) power flow model and investigates the relation among the variation of Internet Quality of Service (QoS) and the variation of the QoS of the electrical network using a data packet model to model the Internet communication layer. Based on this model, they develop a Decision Support System to test mitigation and healing strategies.

3.2.6 Other Approaches

Besides the contributions presented, there are some other approaches to model and simulate the interdependency phenomena among infrastructures. These include the High Level Architecture (HLA) based method, the Petri-net (PN) based method and so on.

HLA is a general purpose architecture for distributed computer simulation systems. Eusgeld et al. [36] proposed a HLA-based interdependency modeling architecture based on three layers: the lower level includes the physical models of single infrastructures, the middle level manages the interactions among models of different infrastructures and the high level represents the overall system model. This approach simulates the interdependencies through a distributed simulation environment through communications among the three layers. Such an approach was used to simulate the interdependencies among a power network and its own SCADA system [35].

Based on the Petri-net (PN) based approach, Laprie et al. [50] developed a petri-net to represent the interdependencies between electricity and communication network whereas Sultana and Chen [82] modeled the effect produced by floods on a set of interdependent infrastructures which exhibit vulnerabilities specified according to fragility curves.

3.3 NETWORK BASED TOOLS

In this Section, we focus on two specific network based tools namely i2Sim and CISIA which were adopted for the impact assessment and the emergency resources allocation problems covered in Chapters 5, 6

and 7. Both tools adopt a flow based approach to model the different resources exchanged among the entities.

i2Sim captures the behavior of infrastructures with matrices that describe how input resources interact to produce a specific kind of resource. Being built under Matlab/Simulink, i2Sim offers a usable graphical user interface to build the interdependency model. Compared to i2Sim, CISIA offers more capabilities to build the model such as the possibility to define different kinds of faults and output resources for each entity and the possibility to model uncertainty through fuzzy variables. However, CISIA lacks usability as the interdependency model should be entirely coded.

3.3.1 *i2Sim*

i2Sim [72] allows to model interdependencies among different critical infrastructures based on a mathematical approach. Components defined in physical layer can interact with the decision-making layer through event forwarding approach.

Such a model is based on the following key components:

- **Production cell:** A production cell is an entity that performs a function. For example, a hospital is a cell that uses input tokens e.g., electricity, water, doctors, and produces an output token e.g., the number of patients treated. Each production cell is associated a table, called Human Readable Table (HRT), that defines how quantities of input resources are combined to produce quantity of output resource.
- **Channel:** A channel is a means through which tokens flow from an entity (e.g., a cell) to another one.
- **Token:** Tokens are goods and services that are provided by some entity to another one that uses them. Such tokens can be electricity, water, medical supplies, etc.
- **Control:** These are Distributor and Aggregator units allowing to change their state based on the events received from the decision making layer. Distributors divide a specific resource among different channels according to specific quantity ratios. Aggregators group resources coming from different channels into one channel.
- **Storage:** Storage cells are able to keep an initial amount of tokens and release them based on an external signal.

Figure 2 shows an example of a production cell modeling a hospital together with its relative Human Readable Table. In the upper part, the hospital operates normally with an output called Resource

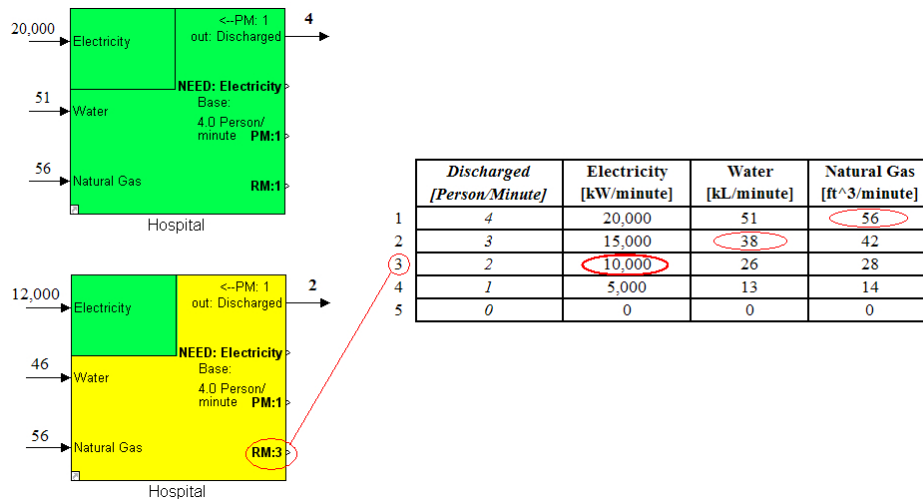


Figure 2: An example of a production cell.

Mode (RM) of 4 patients healed per minute. In the lower part, the resource amounts varied so that the operability of the hospital changes accordingly. In particular, to determine the new RM of the cell and the respective output every input value is located within the working threshold on the corresponding column. Thus, electricity value of 12,000 is associated to the third row, water with 46 to the second row and natural gas to the first row. Electricity is thus the limiting factor and the cell output is thus 2 patients healed per minute.

The generation and flow of tokens among different entities is given by physical capability of each of the cells (e.g., power generation capacity), their environmental constraint (e.g., damage of cells) or human decision factor (e.g., redirection of water supply to a hospital rather than to a resident area). The operational characteristics of each of the cell are provided by a non-linear behavior that is encapsulated within a block through a production cell. This allows to model interdependencies between different infrastructures through non-linear relationships.

In order to establish benchmark cases, i2Sim was applied to study the interdependency phenomena inside the University of British Columbia (UBC) campus that has the properties of a small city [53]. Specific HRT were built based on the input-output relations among the different networks with the support of infrastructure operators. The model allowed to measure the response of the UBC security facilities w.r.t. disastrous events and to test resource allocation policies.

3.3.2 CISIA

CISIA [25] is a modeling framework that considers the overall system of system as being composed of a set of entities produces various resources. In this framework, the different classes of interaction are represented through specific interconnection matrices so that make the overall system can be considered a multigraph allowing the implementation of complex topological and dynamical analyses.

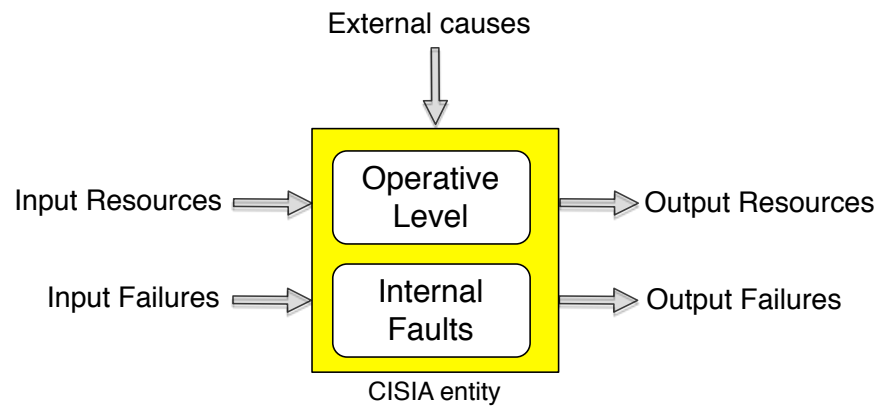


Figure 3: Input-Output representation of a CISIA entity.

Figure 3, represents the components of an entity modeled in CISIA:

- Entities can produce, transport or consume tangible or intangible resources (e.g., goods, services, policies);
- Entities can be affected by faults;
- Faults can be propagated across entities;
- The capacity of each entity to distribute resources depends on its operative level and on the severity of the faults that affect the entity.

Each entity is associated an operative level that represents the state of the entity and can receive input resources and failures that influence, together with the operative level, the capacity to generate resources and failures. External causes representing disruptive phenomena can also reduce the operability level of an entity.

To model the interaction of the agents that provide mutual requirements or disseminate failure, three kinds of matrices have been devised: Operative Level Incidence Matrix, Requirement Incidence Matrix, and Fault Incidence Matrices. Fault incidence matrices allow the analysis of different types of failure propagation (e.g., physical, cyber). In order to represent the uncertainty of human operators interacting or representing entities in CISIA, all the variables describing the dynamics of entities are expressed as Triangular Fuzzy Numbers.

CISIA adopts a discrete-time simulation approach where each simulation step is driven by a clock routine that synchronizes the message exchange among entities. In order to model the different flow rate of resources, it is possible to model delays for the communication channels connecting different entities. At the beginning of each simulation step, different instant cycles are performed, until the system reaches a steady state.

CISIA was effectively used in several research projects [3, 2] to model the interdependencies power distribution grid, the relative SCADA system and the Telecom network allowing the communication between the power grid and the SCADA infrastructures.

3.4 OTHER APPROACHES

In Section 3.2.6, we presented a distributed simulation environment based on HLA to simulate interdependency phenomena.

In the following Section, we present a similar approach based on WebSimP, a platform allowing the simulation of the physical layer of single infrastructures.

3.4.1 *WebSimP*

In this Section, we present Web-Service based simulation platform for critical infrastructures (WebSimP) [11], a distributed environment for the simulation of the behaviour of the electrical and telecommunication domains.

WebSimP is integrated inside the Disaster Response Network Enabled Platform (DR-NEP) [55], a platform enabling decision making for the validation of resource allocation policies.

As shown in Figure 4, DR-NEP is a web service platform that enables different simulators to communicate results to each other via a common enterprise service bus (ESB) and a database. A distributed computing architecture is employed to support decision making. Every simulator is connected to DR-NEP using an adapter that listens on the ESB for instructions about running simulations, gathers inputs from the other simulators and the database and pushes results from the simulators to the database. After the simulators and adapters are configured, a controller in the ESB pushes input to the simulators at predefined intervals. By linking the izSim interdependency simulator (presented in Section 3.3.1) with a power grid and telecom simulator, DR-NEP enables the validation of resource allocation in the electrical domain.

WebSimP enables disaster support systems that are integrated with DR-NEP to be invoked separately through web service technologies. Such a service based platform offers many benefits over other types of

distributed computing architectures in terms of interoperability and ubiquity.

In particular, WebSimP allows the simulation of the electrical and telecommunications domains. Each simulation layer incorporates three software components: (i) a web service that receives operation requests to execute a particular simulation; (ii) a software adapter that implements the details of each requested operation and oversees command execution in the simulator and output data post-processing; and (iii) a simulator (e.g., discrete/continuous, deterministic/stochastic) that executes a simulation model for a certain domain.

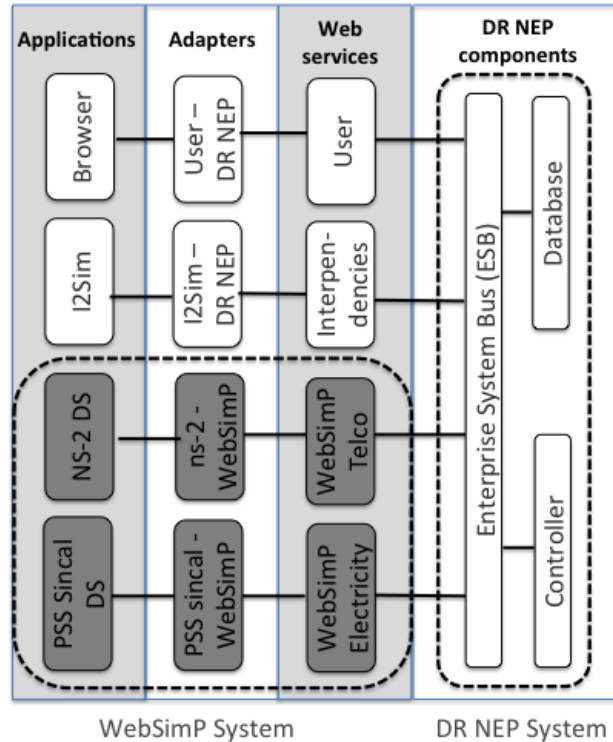


Figure 4: DR-NEP-WebSimP architecture.

Electrical Adapter. The electrical adapter is a software component that is responsible for invoking operations in a pre-existing model. The possible operations are:

- **Disconnection of electrical lines.** Disconnection of a line may simulate a damage event on the power network.
- **Reclosure of breakers.** The operation simulates the closure of breakers that may be needed in case of distribution network reconfiguration.
- **Load flow calculation.** The operation executes a load flow calculation on the power network including information on voltage, current and power.

- **Power load shedding.** The operation sets new values of active and reactive power that a certain load consumes.

The simulator determines the loads that the grid may support without damaging the infrastructure by considering physical limits on parameters such as current and voltage. The PSS Sincal electrical simulator [5] is used; it supports network planning for power transmission and distribution networks (e.g., load flow calculations, dynamics and network protection).

Telecommunication Adapter. The telecommunications adapter is a software component that is in charge of invoking operations in a pre-existing telecommunications simulation model. The possible operations are: (i) network configuration (e.g., disconnecting telecommunications and SCADA elements to simulate damage events); (ii) constraint computation (e.g., communications bandwidth); and (iii) electrical network reconfiguration time computation (e.g., response time required to send and execute specific commands). The telecommunications simulation uses ns-2 [4], a discrete event simulator that allows the modeling and simulation of communications protocols, routing and multicast protocols over wired and wireless networks.

As an application of the DR-NEP-WebSimP platform, in Chapter 7 we present how this platform can support decision making in a scenario with interdependencies existing between a power grid and a supervisory control and data acquisition (SCADA) system.

3.5 CHAPTER SUMMARY

In this Chapter, we presented different approaches for the modeling and simulation of interdependencies among critical infrastructures.

Network based approaches based on networks theory consider critical infrastructures as graphs where each node represents an infrastructure. In these approaches, it is possible to introduce relationships and hierarchies between quantities arriving and leaving the nodes and to model physical states of the nodes.

The fact that many of the relationships between causes and consequences are non-linear is a limiting factor of many of the models considered. In this regard, agent based techniques or non-linear transfer function approaches are usually more flexible.

In addition to being able to represent relationships, physical states, and external events, dynamic (i.e., inertial) states can be modeled in System Dynamics (SD) approaches through the use of differential equations. Being based on discretized states where the current state is a function of past states, dynamic states can also be modeled with CISIA.

We focused on two network based approaches, namely i2Sim and CISIA, and a distributed simulation environment provided by Web-SimP. i2Sim and CISIA are flow based approaches where nodes and

edges are able to produce and distribute the services respectively. WebSimP adapters facilitate the exchange of information between the impact assessment module (based on i2Sim) and the infrastructure simulators, controls the execution of the simulators and calculates the constraints on the loads to insure that they are feasible.

Part II

SITUATION AWARENESS METHODOLOGIES

Data fusion provides means for combining pieces of information coming from different sources and sensors. This can help to enhance the security of critical infrastructure systems (e.g., power grids, water distribution networks) by providing an improved situation awareness that is relevant for decision making.

Usually, critical infrastructure systems combine the information coming from their sensors individually, without sharing any information regarding the state of their functioning with other infrastructures. This originates mainly from the fact that the delivery of sensitive information to third-parties infrastructures can be a security issue, and this has been investigated in several research initiatives [83, 2]. However, during real-time situations, there may be scenarios in which allowing a full exchange of information could be beneficial.

Foglietta et al. [41] applied an algorithm based on Gasparri et al. [42] to share information among a set of critical infrastructures in order to produce common knowledge and decrease the possibility of producing cascading effects. In this framework, the set of infrastructures, or *agents*, constitute a connected network and combine their local information, regarding their functioning state, using a distributed algorithm. However, the approach requires the network topology to form a spanning tree.

Denoeux [30] proposed a distributed algorithm that implements data fusion over an unknown topology. This algorithm computes the confidence of each node, by combining all the data coming from the neighbors, using a *discounted cautious operator* and without relying on a central node for the data collection. Convergence of the algorithm is proved in finite time for any initial configuration and for any unknown network topology. However, this algorithm requires the network topology to become stable, i.e., nodes and links are fixed and

each agent does not perform any dynamic observation, in order to reach convergence.

Considerable research has been conducted to apply data fusion techniques to enhance the security of critical infrastructures.

Flammini et al. [40] proposed a theoretical centralized framework for correlating events detected by a wireless sensor network in the context of critical infrastructure protection. They developed a decision support system to face security threats by collecting data from heterogeneous sources. Genge et al. [43] considered the concept of cyber-physical data fusion using the Dempster-Shafer theory to combine knowledge from the cyber and physical dimensions of critical infrastructures in order to implement an anomaly detection system able to detect possible threats in a centralized fashion. The system was validated in a scenario considering the consequences of Distributed Denial of Service (DDoS) attacks on the information network, and the propagation of such disturbances to the operation of a simulated power grid. Timoen et al. [85] proposed a platform that combines an agent-based brokered architecture and the JDL data fusion model to produce events from different source systems and the brokered architecture allowing the agents and multiple analysis components to collaborate. The current state of the infrastructure can be determined by combining and analyzing event streams. However, generally speaking the centralized nature of these approaches, i.e., all data must be collected by a single node performing the aggregation, renders this approach not robust against single node's failures.

Oliva et al. [61] presented a distributed consensus algorithm based on fuzzy numbers and applied to a case study related to crisis management. The algorithm provides consensus on the overall criticality of a situation based on the information produced by human operators regarding the state of specific infrastructures. However, this approach may require an high complexity in generating appropriate membership functions to model the opinions of the operators.

Sousa et al. [81] described a construct for the protection of critical infrastructures based on distributed algorithms and mechanisms implemented between a set of devices providing secure gossip-based information diffusion among the infrastructures. Although this approach ensures that the traffic data satisfies the security policies of an infrastructure against cyber attacks, it lacks flexibility when dealing with other kinds of threats e.g., physical security threats or when the information of a possible threat is uncertain.

In this Chapter, we advance the state of the art by releasing the typical assumption of static network topology to accommodate for a scenario where link failures may occur (e.g., due to natural disasters or cyber attacks). In particular, we propose two data fusion approaches for critical infrastructure scenarios that use two gossip algorithm proposed by Denoeux [30] to exchange the information among

the infrastructures and thus increasing their situational awareness. We model the failures and threats with the Dempster-Shafer formalism to take into account the imprecision and uncertainty in detecting the possible events without the requirement of specifying membership functions as required by fuzzy-based approaches presented in [61].

In Section 4.1, we present a distributed gossip algorithm [DPGP15] where each all infrastructure is proved to convergence in finite time, without relying on a stable network topology, and using the cautious rule of combination [29] as the aggregation rule. This operator does not require the information sources to be independent or distinct and thus is preferable compared to other ones, e.g., the TBM conjunctive and Dempster rules [28, 79], which, instead, lack robustness when equal information are combined several times. Considering that the cautious rule of combination is appropriate when all sources are considered reliable, we define the convergence response when all sources are non-distinct and reliable.

In Section 4.2, we define a data fusion framework [DPGP15] where the underlying distributed gossip algorithm allows each infrastructure to converge to a specific value so that it is possible to capture the particular behavior of each infrastructure. We provide simulation results showing that each infrastructure reaches convergence in finite time, without relying on a static network topology and where link failures may occur. We use the cautious operator [29] along with a specific evidence discounting function as the aggregation rule among the informational content provided by the different infrastructures. In this framework, when updating the knowledge of one infrastructure, we use the evidence discounting function to decrease the informational content provided by a supporting infrastructure when the considered infrastructure is loosely coupled.

4.1 DATA FUSION USING DISTRIBUTED GOSSIP ALGORITHM

In this Section, we present a data fusion algorithm where the network topology is unknown. Theoretical results show that the algorithm convergence only requires connectedness of the network topology over a certain time window, thus introducing resilience against temporarily faults of the critical infrastructure communication layer.

4.1.1 Data Fusion Algorithm

Let us consider a network of agents described by an undirected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}(t)\}$ where $\mathcal{V} = \{v_i : i = 1, \dots, N\}$ is the set of nodes (agents) and $\mathcal{E}(t) = \{e_{ij}(t) = (v_i, v_j)\}$ is the set of current edges, representing the point-to-point communication channel availability. We denote with t_k the instant when the k -th communication on the network

occurs. Furthermore, the following assumptions on the network of agents are made.

1. The network can be described by a connected undirected graph.
2. Every node produces a local BBA expressed as a weight function called *direct confidence*.
3. Agents communication is asynchronous, that is at every time t_k only a pair of agents (i, j) interact.
4. Each agent i is capable of handling the storage of the current direct confidence and the *edge confidence* computed through the aggregation with a node v_j s.t. $(v_i, v_j) \in \mathcal{E}(t)$.

In the proposed framework, the interaction among the agents can be modeled through a gossip algorithm [14], which is defined as a triplet $\{\mathcal{S}, \mathcal{R}, \epsilon\}$, where the following holds:

1. $\mathcal{S} = \{s_1, \dots, s_n\}$ is the set containing the local states $s_i \in \mathbb{R}^q$ of each agent i in the network s.t. $s_i(t) = (w_i(t, \gamma_1), \dots, w_i(t, \gamma_q))$ at time t with $q = |2^\Omega \setminus \Omega|$
2. \mathcal{R} is the interaction rule based on the \bigotimes operator s.t. for any couple of agents (i, j) with $e_{ij} \in \mathcal{E}(t)$, gives $\mathcal{R} : \mathbb{R}^q \times \mathbb{R}^q \rightarrow \mathbb{R}^q$ s.t.:

$$s_i(t) \bigotimes s_j(t) = (w_{i \otimes j}(t, \gamma_1), \dots, w_{i \otimes j}(t, \gamma_q)) \quad (6)$$

3. ϵ is the edge selection process that specifies which edge $e_{ij} \in \mathcal{E}(t)$ is selected at time t .

A possible implementation of the algorithm is presented in Algorithm 1.

Algorithm 1: Gossip Algorithm

Data: $t = 0, s_i(0) \leftarrow$ initial direct confidence $\forall i \in 1, \dots, N$

Result: $s_i(t_{\text{stop}}) \forall i \in 1, \dots, N$

while *stop_condition* **do**

- Select and edge $e_{ij} \in \mathcal{E}$ according to ϵ ;
- Update the state of the selected agents according to \mathcal{R} :

$$s_i(t+1) = s_i(t) \bigotimes s_j(t)$$

$$s_j(t+1) = s_j(t) \bigotimes s_i(t)$$
- Let $t = t + 1$.

end

It is worth noting that, our algorithm does not require agents to have a unique identifier, that is we do not require the agents to know

the identity of the neighbors they are exchanging information with. Note that, this assumption is not cosmetic as security and confidentiality represent typical requirements for interdependent critical infrastructures [15]. So far, we have introduced the gossip algorithm based on the \mathcal{R} interaction rule. In the following, it will be shown that, if the agents apply the gossip algorithm described previously, over a dynamic network topology where link failures may occur due to natural disasters, cyber attacks or physical-security threats, they will eventually converge toward a common BBA expressed as the weight function $w(\cdot)$ given in (3) under the assumption that connectedness of the network topology can be ensured over time-windows.

4.1.2 Convergence Criteria

Lemma 1. *Let us consider a gossip algorithm $\{\mathcal{S}, \mathcal{R}, \epsilon\}$ over a time-varying graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}(t)\}$ with \mathcal{S} and \mathcal{R} defined previously. Let us assume each agent i at time $t = 0$ provides an independent set of direct confidences described by the weight function values $s_i(0) = \{w_i(0, \gamma_\alpha); \gamma_\alpha \in 2^\Omega \setminus \Omega\}$ obtained from BBA and commonality functions $m_i(0)$ and $q_i(0)$ respectively, through (1) and (3).*

If ϵ is such that $\forall t \exists \Delta t \in \mathbb{R}$ such that $\mathcal{G}(t, t + \Delta t)$ is connected, then there exists a time $t = \bar{t}$ s.t. $\forall t' > \bar{t}, \forall \gamma_\alpha \in 2^\Omega \setminus \Omega$, the following holds:

$$s(t') = s_1(0) \bigwedge s_2(0) \bigwedge \dots \bigwedge s_n(0). \quad (7)$$

that is, each agent i converges toward the same weight function.

Proof. see Section A.1 in Appendix A. □

Lemma 2. *(Convergence time) Let us consider an edge selection policy ϵ such that $\forall t \exists \Delta t \in \mathbb{N}$, so that the $\mathcal{G}(t, t + \Delta t)$ is connected. If exists a time $M \in \mathbb{N} : \Delta t < M \forall t$, then the convergence is reached by any agent at most $t = d \cdot M$, where d is the diameter of the network.*

Proof. see Section A.2 in Appendix A. □

4.1.3 Case Study

As a case study, we consider a scenario of a set of assets, also known as Critical Infrastructures (CI), that are essential for the functioning of a society and economy. The occurrence of specific conditions on such CI, are monitored by a set of n agents. Usually, CI (e.g., power grids, Telecommunication networks, Gas pipeline networks) exhibit various kinds of dependencies (e.g., cyber), which, may lead to cascading failures, i.e., failures that originates in one system and may produce disruptions in other systems.

We consider a set of systems that are geographically distributed, and can generically represent the infrastructures of a city district.

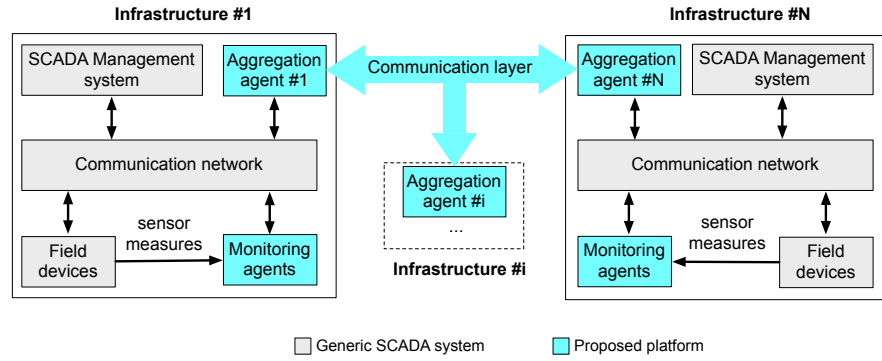


Figure 5: Communication framework among the infrastructures in the considered scenario.

Each infrastructure is monitored by a SCADA system, that allows the correct functioning including:

- The **SCADA Management system** (e.g., HMI, Historian) running in a SCADA control centre to monitor and control the field equipment;
- A **communication network** that allows the exchange of messages between the field devices and the SCADA management system. The communication network may be proprietary or public and based on specific SCADA protocols (e.g., Modbus, Modbus over TCP);
- The **field devices** (i.e., sensors, PLC, RTU, IED) that acquire the physical quantities of the system and implement control actions.

Although critical infrastructures exhibit different kinds of dependencies, usually, they do not share any information. In our scenario, we suppose, on the contrary, that each infrastructure is able to produce information regarding a possible cause of fault. This information, is produced by the monitoring agents of all infrastructures, deployed on the field devices, to detect the most credible cause of fault or threat, and exchanged among the agents to produce the same knowledge. The information sharing may be also realized in real scenarios by implementing specific policies among infrastructures.

In our scenario, the information to be shared among the infrastructures is provided by two kinds of agents, as shown in Figure 5:

- **monitoring agents** acquiring measurements from the field devices. Such agents can raise specific alarm conditions to detect: (i) physical events (e.g., the fault of a valve in water supply system); (ii) cyber events (e.g., an intrusion on a RTU of power distribution system), and (iii) physical-security events (i.e., the access of unauthorized personnel in the area of system under control, which may sabotage a system).

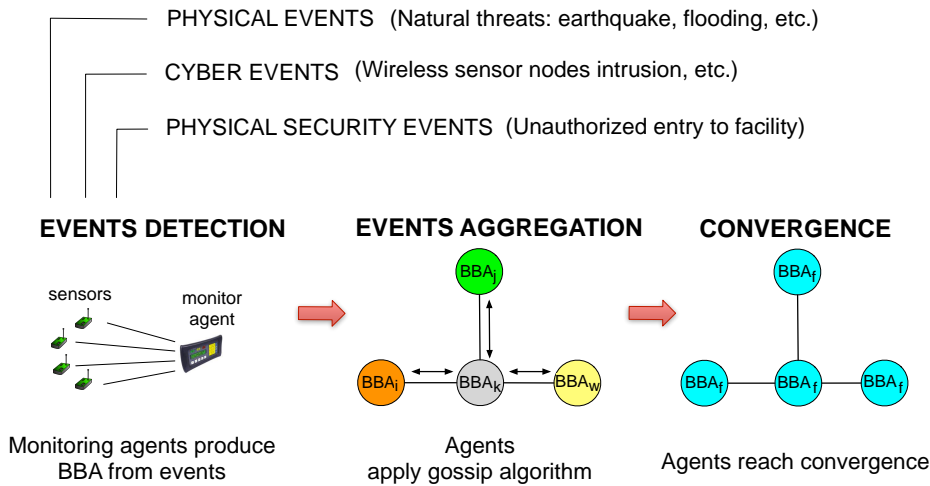


Figure 6: Communication framework among the infrastructures in the considered scenario.

- **aggregation agents** impersonating the SCADA Management system. They cannot correlate events from the field devices, but act as aggregation nodes only by collecting the information of the neighbor monitoring agents, and distributing such information to other peer-agents of other infrastructures.

The resulting system, can be modeled as a multi-agents platform for distributed data aggregation, where, each agent, can produce a BBA expressing the possible cause generating a critical event, which, can affect the functionality of each infrastructure.

The monitoring agents, revealing physical and cyber events, are connected to the aggregation agents through the SCADA communication network of each infrastructure. The monitoring agent detecting physical-security events is impersonated by a *security patrol*, that is shared among infrastructures to detect wireless intruders with a dedicated device, that are in proximity of the monitored infrastructures. Such a monitoring agent may issue an alarm condition through a wireless communication with the nearest infrastructure communication network, in order to alert about a possible physical-security threat. Every agent is able to run the algorithm presented in Section 4.1.1, in order to evaluate the direct confidence and to communicate with the neighbor nodes. The communication among the aggregation agents is based on Virtual Private Network (VPN) links (represented by links 8..12 in Figure 7). Based on our assumptions on aggregation agents, the latter, act as aggregation nodes only (i.e., their direct confidence depends only on the neighbour nodes).

In Figure 6, we describe three main phases relative to the agents' interaction:

- **Events detection:** the monitoring agents use measurement coming from the sensors to produce a BBA from specific events. For

instance, agents acquiring measurements from seismic sensors or pluviometers, can provide an early warning against possible faults in the systems monitored, which, may be induced by earthquakes and floods.

- **Events aggregation:** monitoring and aggregation agents fuse their information based on the underlying data aggregation algorithm.
- **Convergence:** monitoring and aggregation agents reach convergence in a finite time step and exhibit the same belief associated to the most credible cause(s) of fault.

It is worth noting that, based on *Lemmas 1* and *2*, the convergence of the algorithm is ensured for any edge selection policy ϵ that allows to obtain a connected graph in finite time. The latter property is particularly important in a disaster environment, such as the scenario described, where the communication path among two nodes may be unavailable over time, due to different reasons: (i) physical destruction of network infrastructure components (e.g., caused by a natural disaster or a terroristic attack); (ii) disruptions in supporting infrastructures (e.g., due to the lack of electrical power in telecommunication equipment); (iii) disruption due to congestion (e.g., due to cyber attacks such as Denial of Service attacks). Indeed, the loss of one or more nodes, that can modify the agents' topology, will not affect the convergence of the algorithm, provided that the topology remains connected over time. Moreover, as the security patrol is moving, its link with peer-aggregation agents, may change over time. For the sake of simplicity, we assume that the security patrol is connected to only one aggregation agent for each time step. Anyway, based on *Lemma 1*, the violation of this assumption, would not have any effect on the convergence of the algorithm.

The presented approach is distributed as it can be implemented in a network without a central node. This differs w.r.t. a centralized approach, that, instead, is typical in traditional SCADA system architectures. In particular, in a centralized approach, the SCADA management system would be able to gather and correlate events and security information coming from the field equipment, to reveal malicious activities that are perpetrated in a distributed manner. In other words, the presence of a centralized node would be able to produce more accurate information about the state of the monitored system. Our approach is distributed, because, the innovative SCADA management system nodes, impersonated by aggregation agents, act as neutral nodes with an initial BBA s.t. $m(\Omega) = 1$. Such nodes, become informational when they perform an aggregation with other (informational) agents.

Indeed, a distributed approach may present several advantages compared to a centralized one when considering a disaster scenario.

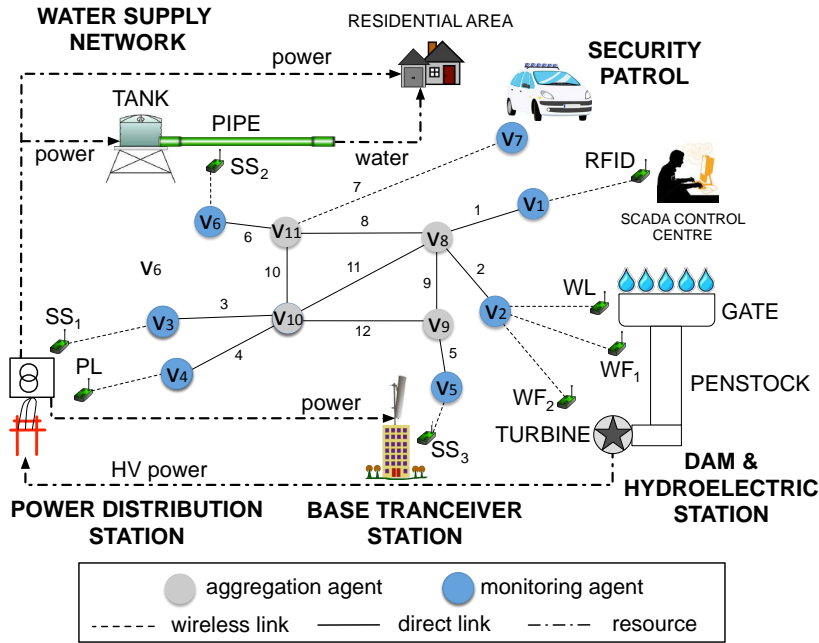


Figure 7: Sample scenario.

One advantage is concerned with more reliability: a distributed approach, being based on a plethora of monitoring agents, relies on many agents instead of only one node, which, may be out of service or isolated following an earthquake. In addition, during an emergency time, it may be preferable to provide information timely, even if less informative, instead of waiting for more accurate information, that can be given by a centralized approach.

4.1.3.1 Problem Formulation

We consider $n = 4$ interdependent critical infrastructures, that can be affected by failures or threats. Each infrastructure is able to produce one or more BBAs from physical, cyber and physical-security events detected by monitoring agents. The frame of discernment is $\Omega = \{a, b, c, d\}$ where a denotes a possible physical failure, b a possible cyber intrusion or attack, c a possible physical-security threat, and d a normal functioning level.

Figure 7 shows the scenario involving a dam, which feeds a hydroelectric power station, which feeds a power distribution substation through a transmission network (not modeled for simplicity). A Base Transceiver Station (BTS), providing telecommunication services to a city district, receives electricity from the power distribution station. The dam provides water to the hydroelectric power station through a gate that is remotely controlled to release basin water and activate the power plant turbine. To feed the water pumps and the automation de-

Table 3: Monitoring agents considered in the scenario.

Dam & h.s.	Power d.s.	BTS d	Water d.s.	Security patrol
v_1, v_2	v_3, v_4	v_5	v_6	v_7

vices, the water supply network, receives electricity from the power distribution station. Failures occurring in the considered infrastructures, may produce disruptions for the population and the economic sector of a city district.

Table 3 presents the monitoring agents considered for each infrastructure. In the following, we present practical methods that can be implemented by the agents, to generate the relative BBA from sensor measurements, in the considered scenario. Then, we show how the algorithm converges, in a limited time, considering an initial set of BBAs.

4.1.3.2 Dam and Hydroelectric Power Station

The dam and hydroelectric power station are controlled by a SCADA system that utilizes a wireless sensor network. Water fed to the hydroelectric power station, is conveyed through pipes called penstocks.

Agents v_1 monitors possible unauthorized physical access in the SCADA control room of the dam. In particular, the agent receives information via wireless from an RFID (Radio Frequency Identification) door sensor installed in the SCADA control room, to alert about the possible intrusion of unauthorized personnel, which may compromise the functioning of the dam. The occurrence of this condition is not regarded as a high credibility level of a physical-security threat since the SCADA control room door could be opened by a different employee when authorized personnel entered the room. However, when modeling the BBA of agent 1, we consider the possibility that, an intruder, with access to the SCADA control room, may be facilitated to perform a cyber attack (see Table 17).

Agents v_2 periodically monitors the water flow rates and the water levels, measured by sensors, and use them to verify the violation of security conditions that may anticipate the malfunctioning of the turbine control [46]. In fact, in a generic dam working in normal conditions, two conditions hold: (C1) the difference between the water flow rate, measured by two water flow sensors, located at the extremes of the penstock (WF_1 and WF_2 in our scenario), should vanish in about three seconds, and (C2) the variation of the water level into the basin of the dam (measured by the WL sensor in our scenario), should be consistent with the variation of the incoming and outgoing water flow. Although the violation of each individual condition cannot be regarded as a consequence of a cyber attack, but rather a physical failure, the violation of both conditions, can increase the credibility level

Table 4: BBA generated by agent v_1 .

A	$m_1(A)$	
	door closed	door opened
d	0.9	-
ac	-	0.3
bc	-	0.4
abc	-	0.2
Ω	0.1	0.1

Table 5: BBA generated by agent v_2 .

A	$m_2(A)$			
	C_1, C_2	$\neg C_1, C_2$	$C_1, \neg C_2$	$\neg C_1, \neg C_2$
d	0.9	-	-	-
ab	-	-	0.2	0.3
ac	-	0.3	0.1	-
ad	-	0.1	0.5	-
bc	-	0.2	-	0.5
abc	-	0.1	-	-
Ω	0.1	0.3	0.2	0.2

in revealing a cyber attack. A possible attack scenario, can be implemented by an attacker that compromises the water flow sensors, in order to hide the changes in the water flow rate in the penstock. With this in mind, we modeled the BBA associated to agent v_2 , by combining the verification/violation of the two security conditions (see Table 18).

4.1.3.3 Power Distribution Station

Earthquakes and hurricanes are known to produce a devastating effect on power distribution systems [63]. In general, earthquakes, could damage all types of power system equipment causing interruptions that may last some days. To this aim, usually, in power distribution station buildings, reinforced concrete, fire- and explosion-resistant walls or barriers, are installed between major pieces of equipment, such as transformers, circuit breakers, and regulators. Hurricanes, can be followed by torrential rains, and can affect distribution systems more heavily than generation and transmission. Floods induced by heavy rainfall, can damage the low lines of a power distribution system and cause power disruptions. Agents 3 and 4 provide early

Table 6: BBA generated by agents v_3 and v_5 .

A	$m_3(A)$					
	$f_d = 0$	$f_d = 1$	$f_d = 2$	$f_d = 3$	$f_d = 4$	$f_d = 5$
a	-	-	-	-	0.3	0.7
d	0.9	0.4	-	-	-	-
ab	-	0.3	0.4	0.5	0.6	0.2
ac	-	-	0.1	0.2	-	-
ad	-	-	0.2	-	-	-
Ω	0.1	0.3	0.3	0.3	0.1	0.1

warning regarding possible physical faults, induced by seismic events and floods, respectively.

Agent v_3 acquires peak ground accelerations (PGA) from the seismic sensor SS_1 installed in the substation building, and estimates the credibility of a physical fault on the power distribution station, based on the structural properties of the building. We assume the following properties for the building: (i) is a reinforced concrete construction; (ii) has one storey and (iii) is a recent construction. These properties can be associated to a seismic vulnerability index I_v (ranging from -6 to 60), s.t. $I_v = 0$. Agent v_3 transforms the PGA of a seismic event, revealed by the seismic sensor, into a Microseismic intensity index I_{MCS} , through the following relation, defined by Decanini et al. [26], valid for a building with the properties mentioned:

$$\log \text{PGA} = 0.594 + 0.197I_{MCS} \quad (8)$$

Then, let us consider following relations, defined in [44], that relate I_{MCS} and I_v to the mean damage d for the building (ranging from 0 to 5), and the corresponding factor of damage f_d (ranging from 0 to 1), respectively:

$$d = 0.5 + 0.45(\arctan(0.55(I_{MCS} - 10.2 + 0.05I_v))) \quad (9)$$

$$f_d = d^{1.75} \quad (10)$$

Based on these relations, and the I_{MCS} and I_v values calculated, agent 3, can calculate the factor of damage f_d (Figure 8) and estimate the credibility of a physical fault affecting the power distribution station. Table 13 shows a possible implementation of the BBAs for the agent v_3 , based on the factor of damage f_d .

Agent v_4 estimates the real-time strength of a current rain precipitation, measured by a pluviometer sensor located in the substation, to estimate the possible effects of floods on the functionality of the substation. To this regard, a hot-spot analysis was conducted over






LEVEL 1: slight	LEVEL 2: medium	LEVEL 3: severe	LEVEL 4: very heavy	LEVEL 5: collapse		
						
Levels of Damage	0	1	2	3	4	5
Factor of Damage (f_d)	0	0.01	0.1	0.35	0.75	1

Figure 8: An example of expected damage scenario ([44] and [69] modified).

Table 7: BBA generated by agent v_4 .

A	$m_4(A)$			
	$Q \leq 20$	$20 < Q \leq 35$	$35 < Q \leq 50$	$Q > 50$
a	-	-	-	0.6
d	0.9	0.3	-	-
ab	-	0.5	0.4	0.2
ac	-	-	0.1	-
ad	-	-	0.2	-
Ω	0.1	0.2	0.3	0.2

a 4-years period for a residential urban context. A linear regression analysis was performed between the average disconnections rate of a set of 1266 electrical substations and the quantity of rain precipitation occurred in the area of the substations. Data relative to the rain precipitation was provided by a pluviometer installed in the surroundings of the substations. In order to find a general pattern, we extended our analysis to a high number of substations as the number of disconnections of only one substation was low to generalize the results.

Figure 9 presents the result of regression analysis, that shows a high correlation between the disconnections and the rain precipitations abundance. This result suggests that the precipitation rain quantity may be a reliable predictor of the disconnections and provides a metric to implement the BBAs of agent v_4 . Table 14 presents different credibility levels of physical fault occurring in the considered substation, based on the daily quantity of rain precipitation denoted by Q (mm).

4.1.3.4 Base Transceiver Station

Today, a large number of BTS antennae is installed in the cities, and they are often located on the roof of buildings. This makes such systems being vulnerable to earthquakes, since a damage on a building where a BTS is installed, may generate disruptions on the Telecommunication system causing the lack of communication for the users in the area covered by that BTS. With this in mind, we can model

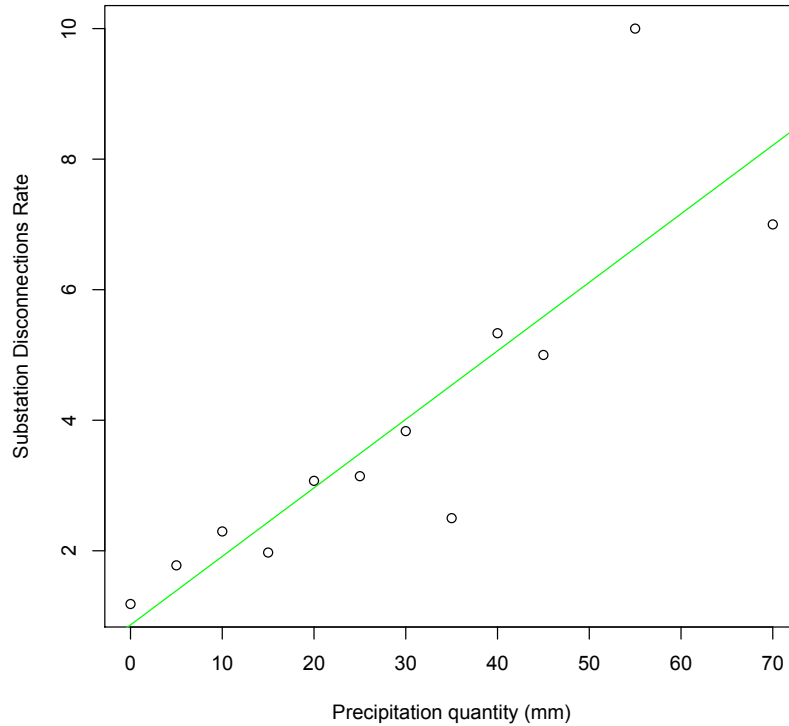


Figure 9: Linear regression between the average disconnections rate and the quantity of rain precipitation.

agent v_5 to acquire peak ground accelerations (PGA) from the seismic sensor SS_2 , installed in the building where the BTS antenna is located, to estimate the possible damage on the BTS, based on the structural properties of the building. Following the approach described in the previous Section, we consider a building with the same structural properties except for the number of storeys that we suppose to be five (to be consistent with common installations of BTS antennae). These properties can be associated to a seismic vulnerability index $I_v = 20$ (see eq. 9, 10). We associate agent v_5 , the same BBAs considered for agent v_3 , in order to relate the damage level of the building to the possible occurrence of a physical failure on the BTS.

4.1.3.5 Water Supply Network

Earthquakes are the most serious natural threat to a water supply network. In particular, earthquakes can cause different damages to pipelines (e.g. longitudinal and circumferential cracks, compression joint breaks) which can provide severe disruptions for water consumers (e.g., residents, hospitals, industrial plants). To detect the effects of seismic events on the water supply network, agent v_6 acquires PGA from the seismic sensor SS_3 installed in a pipeline that serves a residential area. From a structural point of view, we assume to monitor a segmented pipeline i.e. a brittle iron pipeline with bell-and-

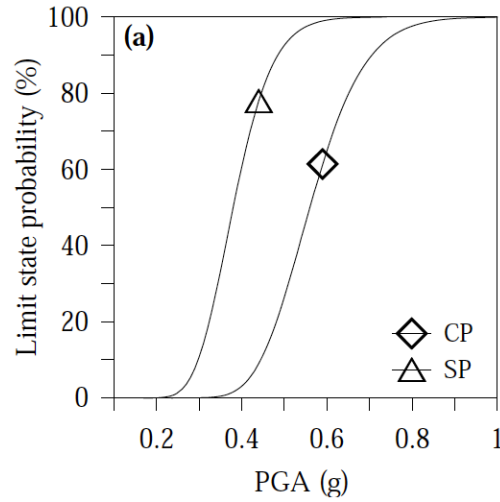


Figure 10: Fragility curve for the segmented pipeline [49].

Table 8: BBA generated by agent 6 (P denotes PGA).

A	$m_6(A)$				
	$P \leq 0.2$	$0.2 < P \leq 35$	$35 < P \leq 50$	$35 < P \leq 50$	$P > 50$
a	-	-	-	0.3	0.7
b	-	-	-	-	-
d	0.9	0.5	0.1	-	-
ab	-	0.3	0.5	0.5	0.2
ac	-	-	0.2	0.1	-
bc	-	-	-	-	-
Ω	0.1	0.2	0.2	0.1	0.1

spigot joints, that is generically used for water supply networks. To define the BBAs generated by agent v_6 , we considered the fragility curve for the specified pipeline, defined by Lanzano et al. [49], and shown in Figure 10. Table 8 shows the credibility values of a physical fault, that are proportional to the severity of the PGA detected during an earthquake.

4.1.3.6 Security Patrol

The security patrol impersonated by agent v_7 , can be based on the security vehicle prototype presented in [65]. This vehicle has specific equipment for detecting wireless threats based on a technique known as Wardriving. This technique can be implemented by a vehicle that drives around a sensitive facility, to collect wireless network traffic, that, may be produced by intruders that are in proximity a specific site. These data are then analyzed to discover potential

Table 9: An example of initial BBAs for agents v_i with $i = 1..11$ at time $t = 0$ and convergent BBA at time $\bar{t} = 106$.

BBA	\emptyset	a	b	c	ab	ac	ad	bc	abc	Ω
$m_1(0)$	-	-	-	-	-	-	-	-	-	1
$m_2(0)$	-	-	-	-	-	0.3	0.1	0.2	0.1	0.3
$m_3(0)$	-	-	-	-	0.5	0.2	-	-	-	0.3
$m_4(0)$	-	-	-	-	0.4	0.1	0.2	-	-	0.3
$m_5(0)$	-	-	-	-	0.5	0.2	-	-	-	0.3
$m_6(0)$	-	-	-	-	0.5	0.3	-	-	-	0.2
$m_7(0)$	-	-	-	-	-	-	-	0.3	0.4	0.3
$m_i(0), i = 8..11$	-	-	-	-	-	-	-	-	-	1
$\bar{m}(\bar{t})$	0.22	0.41	0.06	0.03	0.12	0.08	-	-	0.04	0.04

threats. When a threat is revealed, specific security procedures may be adopted. Due to its specific capabilities, this vehicle can account for cyber and physical-security threats. However, defining a BBA policy for this agent, is application-dependent as it requires a deep analysis of the environment monitored by the car and the wireless traffic data. Indeed, to quantify the credibility of cyber and physical-security threats in a BBA, several properties should be considered, including: (i) the signal strength of the emitter, and (ii) the number of packets collected. Hence, the stronger the signal, the more likely the location of potential intruders will be accurate. Moreover, the more packets are collected, the more likely cyber attacks can be discovered. For our scenario, we suppose to have a security patrol, such as the one presented, that is able to issue, at each time step, cyber and physical-security threats in terms of a BBA. This information is periodically communicated, via wireless connection, to the aggregation agent of a specific infrastructure.

4.1.3.7 Numerical Example

In this Section, we present results of an algorithm execution, where we considered a specific set of BBAs and a random topology generated at each time step. In order to prove the convergence of the algorithm, based on *Lemma 1*, the edge selection policy ϵ , at each time step, generates a random connected graph, where the edges among the agents may, or may not, exist and the security patrol is connected to an aggregation agent that changes over time. This policy is compliant with our assumptions of applying the algorithm in a disaster scenario where the communication network may undergo temporary or permanent disconnections. We consider, at time $t = 0$, the set of

BBAs reported in Table 9, relative to the network topology shown in Figure 7. In particular, we assumed that the security patrol provides the same alarm condition over time when it monitors the water supply network, given by agent m_7 in Table 9, whereas it provides no information, i.e., $m(\Omega) = 1$, when it monitors other infrastructures. Last row of Table 9, shows the convergent BBA $\bar{m}(\gamma_a)$ at time $\bar{t} = 106$, that is obtained from the weight function $\bar{w}(\gamma_a)$.

The BBA $\bar{m}(\gamma_a)$ exhibits as highest credible value the occurrence of a physical fault affecting the considered infrastructures. Anyway, in order to associate a probability measure to each specific event, the pignistic probability defined in (5) may be used to transform the convergent normalized BBA $m(\cdot)$ into a probability measure.

It is worth noting that the same convergent BBA can be obtained through a centralized approach where all BBAs, expressed as weight functions, are aggregated using the cautious operator.

4.2 DATA FUSION USING DISTRIBUTED GOSSIP ALGORITHM WITH EVIDENCE DISCOUNTING

In this Section, the data aggregation algorithm considered allows each infrastructure to converge to a specific value that dependent on the degree of coupling.

Our approach is based on the theoretical framework of Rinaldi [74] (see Section 3.1) and addresses the following dimensions: (i) coupling characteristics (tight or loose); (ii) type of failure (cascading, common cause or escalating failures); and (iii) state of the operation (normal or stressed).

Regarding the approaches aiming at modeling and simulating the dynamic behavior of the infrastructures, we adopted concepts of network-based approaches (see Section 3.2.5) where nodes and edges constructing the infrastructure topologies have the capacities to deliver (or load) services or resources towards (from) other nodes.

Following this approach, in our model the infrastructures are represented by nodes whereas the links represent the communication channels that allow the exchange of information regarding the possible cause(s) of faults. The resulting information sharing produces a higher informative content at each infrastructure layer regarding the possible evolution of the state of operation of each infrastructure.

Each infrastructure i , when fuses its information with the information coming from an infrastructure j , will "discount" the incoming information through a data fusion technique known as evidence discounting according to the degree of coupling among the infrastructure i w.r.t. infrastructure j . In other words, information coming from loosely (tightly) coupled infrastructures is considered less (more) relevant than those coming from tightly (loosely) coupled infrastructures in order to mimic the fact that the state of the operation of the incom-

ing infrastructure would have small (large) effect on the supported infrastructure.

Fusing information between two infrastructures requires to know the degree of coupling among them. In real cases, statistical approaches based on the analysis of historical data relative to the number of disruptions initiated in one infrastructure that resulted in cascading failures may provide evidence that two infrastructures are more or less tightly (or loosely) coupled. Van Eeten et al. [89] conducted an analysis about infrastructure disruptions events gathered from public media occurring in The Netherlands in the period 2010-2014. The analysis considered the main critical infrastructures of The Netherlands and shows that, depending on the infrastructure where the cascading-initiating failures occur, there are infrastructures that, on average, are more frequently affected by cascading failures w.r.t. others. For example, when considering Health as the affected sector, the 50% of the cascading-initiating failures occur in the Energy sector, the 13% in the Telecommunications and the Water sectors and the 25% depend on internal failures.

4.2.1 Data Fusion Algorithm

We aim for a model which represents the interdependencies and the communication channels existing among the different critical infrastructures through a graph structure. This model embeds the notion of degree of coupling based on the general Rinaldi model [74] and on our specific assumptions described in the previous Section.

4.2.1.1 Motivation

To motivate the choice of our model, let us consider a sample scenario. We consider $n = 5$ dependent critical infrastructures, that can be affected by failures or threats. Each infrastructure is able to produce one BBA, expressed as a weight function $w(\cdot)$ from physical and cyber events detected by the aggregation agents. The frame of discernment is $\Omega = \{a, b, c\}$ where a denotes a possible physical failure, b a possible cyber intrusion or attack, and c a normal functioning level.

We consider a set of systems that are geographically distributed, and can generically represent the infrastructures of a city district. The scenario is similar to the one presented in Section uniform where a hydroelectric power station feeds a power distribution station through a transmission network and a BTS which provides telecommunication services required by the SCADA system of the power distribution station and the water pumping station. The BTS receives electricity from the power distribution station. To feed the water pumps and the automation devices, the water pumping station receives electricity from the power distribution station. Failures occurring in the considered

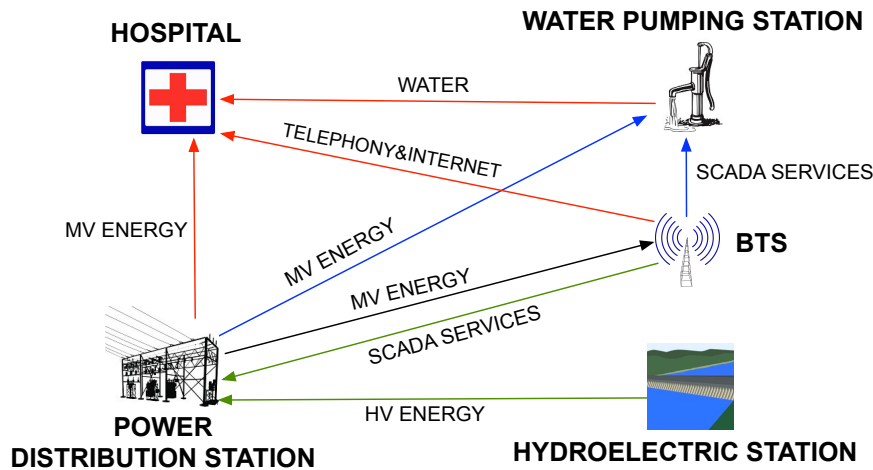


Figure 11: Sample scenario: resources exchanged among the infrastructures.

infrastructures may produce disruptions for a hospital that receives water from the water pumping station and electricity from the power distribution station. In addition, the hospital may suffer disruptions in case of malfunctioning of the Telco BTS, which provides mobile communications to it. Figure 11 shows the dependency layer of the considered scenario. We assume that the infrastructures can exchange information regarding possible failures or threats. The communication is based on Virtual Private Network (VPN) links implemented among the infrastructures that exhibit a non-negligible dependency.

4.2.1.2 Weighted Digraphs to Model Interdependencies

Formally, the model is represented by a weighted digraph \mathcal{G} with vertex set $\mathcal{V} = \{v_1, \dots, v_n\}$, $n > 1$. We assume that \mathcal{G} has no loops. Let $\mathcal{E}(t) = \{e_{ij}\}$ be the set of edges and $\mathcal{Q} = \{q_{ij}\}$ with $q_{ij} \in \mathcal{P} = \{l, m, h\}$ be the set of weights indices associated to each arc e_{ij} in \mathcal{G} .

The different sets of \mathcal{G} are described in the following:

- \mathcal{V} is the set of agents v_i associated to each infrastructure;
- $\mathcal{E}(t) = \{e_{ij}\}$ is the set of edges representing a non-negligible degree of coupling among the infrastructures v_i and v_j ;
- $\mathcal{Q} = \{q_{ij}\}$ is the set of weights indices representing the degree of coupling of infrastructure v_j on infrastructure v_i .

The graph \mathcal{G} represents the *dependencies layer* where each infrastructure or *agent* v_j , by combining its direct confidence with the confidence of all the dependent agents v_i , obtains a *distributed confidence* that expresses the operative level of v_j . Note that for the sake of simplicity, we abstract away from technical aspects concerning how the communication is realized. More precisely, we simply assume the

graph \mathcal{G} encoding the network dependence can be supported by the communication layer. That is, a communication can always be established for each pair of nodes v_i and v_j with coupling w_{ij} if and only if a non-negligible dependence exists, that is $e_{ij} \in \mathcal{E}(t)$.

Furthermore, the following assumptions on the network of agents are made: (i) the graph \mathcal{G} has at least a rooted spanning tree; (ii) every node $v \in \mathcal{V}$ produces a local BBA expressed as a weight function $w(\cdot)$ called *direct confidence*; (iii) nodes communication is asynchronous, that is at every time t_k only a pair of agents (i, j) interacts; and (iv) each agent is capable of storing the current direct confidence, the direct confidence of the ancestors and the *distributed confidence* computed through the nodes aggregation.

4.2.1.3 Agents Interaction

In the proposed framework, the actions among the agents can be modeled through a gossip algorithm [14], which is defined as a triplet $\{\mathcal{S}, \mathcal{R}, \epsilon\}$, where the following holds:

- $\mathcal{S} = \{s_1, \dots, s_n\}$ is the set containing the local states $s_i \in \mathbb{R}^q$ of each agent i in the network s.t. $s_i(t) = (w_i(t, \gamma_1), \dots, w_i(t, \gamma_q))$ at time t with $q = |2^\Omega \setminus \Omega|$
- \mathcal{R} is the interaction rule based on the cautious operator \otimes and the discounting function $r(\cdot)$ s.t., for any couple of agents $v_i, v_j \in \mathcal{V}$ with $e_{ij} \in \mathcal{E}(t)$, gives $\mathcal{R} : \mathbb{R}^q \times \mathbb{R}^q \rightarrow \mathbb{R}^q$ s.t.:

$$s_j(t) = (w_j(t, \gamma_1) \otimes r(w_i(t, \gamma_1)), \dots, w_j(t, \gamma_q) \otimes r(w_i(t, \gamma_q))) \quad (11)$$

$$r(w_i(t, \gamma_a)) = \begin{cases} r_l(w_i(t, \gamma_a)) = \min(1, w_i(t, \gamma_a) + 0.4), & q_{ij} = l \\ r_m(w_i(t, \gamma_a)) = \min(1, w_i(t, \gamma_a) + 0.25), & q_{ij} = m \\ r_h(w_i(t, \gamma_a)) = w_i(t, \gamma_a), & q_{ij} = h. \end{cases}$$

- ϵ is the edge selection process that specifies which edges e_{ij} are selected at time t .

When updating the generic agent v_j with an incoming agent v_i , a discounting function $r(\cdot)$ is applied to the weight function $w_i(\cdot)$ according to the degree of coupling of v_j on v_i . Note that the choice of the discounting function is generally application-dependent. The function given above represents an effective choice for the case study of interest. Note that, when the degree of coupling is high ($q_{ij} = h$) the discounting function leaves the $w_i(\cdot)$ unchanged whereas when the coupling is medium or loose ($q_{ij} = m$ or $q_{ij} = l$ respectively), the

Algorithm 2: Gossip Algorithm**Data:** $t = 0, s_j(0) \leftarrow$ initial direct confidence $\forall j \in 1, \dots, N$ **Result:** $s_j(t_{\text{stop}}) \forall i \in 1, \dots, N$

```

while stop_condition do
  for each edge  $e_{ij} \in \mathcal{E}(t)$  according to  $\epsilon$  do
    Update the state of agent  $j$  according to  $\mathcal{R}$ :
    if  $q_{ij} = l$  then
      |  $s_j(t+1) = s_j(t) \otimes r_l(s_i(t))$ 
    end
    else
      if  $q_{ij} = m$  then
        |  $s_j(t+1) = s_j(t) \otimes r_m(s_i(t))$ 
      end
      else
        if  $q_{ij} = h$  then
          |  $s_j(t+1) = s_j(t) \otimes r_h(s_i(t))$ 
        end
      end
    end
  end
  Let  $t = t + 1$ .
end

```

Table 10: BBA $m_i^f(0)$ applied to node v_i in case of link failure of e_{ij} .

BBA	\emptyset	a	b	c	ab	ac	bc	Ω
$m_i^f(0)$	-	0.10	0.10	-	0.40	-	-	0.40

discounting function applies a decreasing constant factor to the $w_i(\cdot)$. This way, the refined $r(w_i(\cdot))$ approaches to the neutral element w_{\perp} (vector consisting of some $\mathbf{1}$ only) w.r.t. the cautious operator in order to implement low couplings.

In order to make the algorithm robust against communication link failures, when the edge selection process ϵ extracts one or more links e_{ij} that are unavailable at a certain time t , the algorithm associates the BBA $m_i^f(\cdot)$ to the nodes v_i that cannot communicate with the node v_j that performs the update. The BBA $m_i^f(\cdot)$, reported in Table 10, implements a worst-case policy that increases the credibility of failures a and b when no information about the state of operation of an infrastructure v .

A possible implementation of the algorithm, that extends the formulation proposed by Denoeux [29], is presented in Algorithm 1.

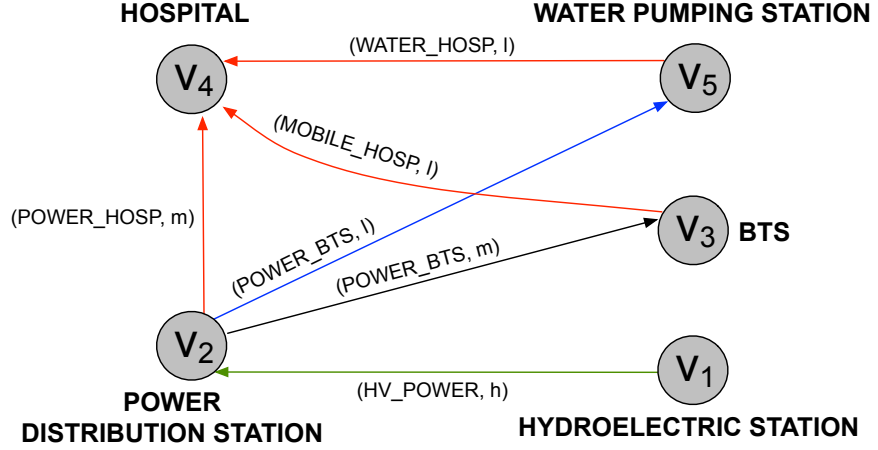


Figure 12: Sample scenario: dependency layer graph \mathcal{G} . Values l, m, h stand for low, medium and high degree of coupling respectively.

4.2.1.4 Graph Construction

Based on the model and the test case that we introduced, we build a graph \mathcal{G} with $n = 5$ agents where each agent models a specific infrastructure and each link models the dependency between two infrastructures.

Regarding the assignment of weights to our case study, we considered the data of the incidents analysis collected by Van Eeten et al. [89] and applied the method based on the occurrence of historical cascading faults described in Section 2. For each infrastructure i , let $R_j = \frac{N_j}{N_i}$ be the number of historical faults N_j initiated in j which produced a fault on i calculated over the total number of cascading failures N_i affecting i . For each dependency among i and j , we assume four cases: (i) $q_{ij} = h$ when $R_j \geq 80\%$; (ii) $q_{ij} = m$ when $80\% > R_j \geq 20\%$; (iii) $q_{ij} = l$ when $20\% > R_j \geq 5\%$; and (iv) a negligible dependency (not modeled as an edge) when $R_j < 5\%$. Considering that there was no mention of the cascading failures occurring among the different infrastructures of the energy sector, we decided to associate a high dependency of the power distribution station on the hydroelectric station and considering this as an autonomous system. Figure 12 shows the corresponding graph \mathcal{G} where each edge is labeled with the service provided and the relative degree of coupling. The resulting system can be modeled as a multi-agents platform for distributed data aggregation where each agent produces a BBA expressing the possible critical event(s) and interacts with other agents through a communication channel.

4.2.2 Simulation Results

In this Section, we present simulation results of the algorithm obtained considering two scenarios: (i) the network topology \mathcal{G} is stable i.e., the set of agents \mathcal{V} and the set of edges \mathcal{E} are both static; (ii) the network topology \mathcal{G} is dynamic i.e., the set of agents \mathcal{V} is static and the set of edges \mathcal{E} can vary on time. For each of these scenarios, we considered two cases: (i) the direct confidence produced by each agent is static; (ii) the direct confidence produced by each agent can vary on time. Regarding the case where the network topology is dynamic, we assume that, at each time step, the graph \mathcal{G} is connected and exhibits at least a rooted spanning tree. In order to provide an indication of the simulation results obtained for each considered case, we use the pignistic measure (see Section 2.4.4) to quantify the probability of occurrence of the operational states of the infrastructures.

4.2.2.1 Static Topology

In this section, we describe the first scenario (static topology) considering the case of both static and dynamic direct confidences for the agents.

Time-unvarying confidences. Consider a stable network topology \mathcal{G} where the set of agents \mathcal{V} and the set of edges \mathcal{E} are both static and the direct confidences produced by the agents do not change over time. Table 17 shows the simulation results in terms of convergent BBAs obtained at time $\bar{t} = 5$ and based on a specific set of BBAs for the system of 5 agents at time $t = 0$. The results show that agent v_4 , that monitors the hospital, starts from a probability of normal functioning $P_{m_4}(t = 0) = 0.55$ and reaches a lower probability of normal functioning $P_{m_4}(t = 5) = 0.38$. This can be explained by the water pumping station and the power distribution grid maintain a stable normal functioning level over time.

Time-varying confidences. Consider a stable network topology \mathcal{G} where the set of agents \mathcal{V} and the set of edges \mathcal{E} are both static and the direct confidences produced by the agents can change over time i.e., the agents can perform dynamic observations over time. Table 18 shows the simulation results in terms of convergent BBAs obtained at time $\bar{t} = 43$ and based on a specific set of BBAs obtained by the system of 5 agents through dynamic observations of agents v_2 and v_3 occurring at time $t = 40$. The results show that agent v_4 , starts from a probability of normal functioning $P_{m_4}(t = 0) = 0.55$ and reaches a lower probability of normal functioning $P_{m_4}(t = 43) = 0.29$. This can be explained by the electrical power, which decreases its credibility of normal functioning. We also discovered that, if the direct confidences change at times t' with $t' > \bar{t}$ where \bar{t} is the convergence time before the dynamic observations occur, the edge selection policy does not influence the convergent BBAs. Instead, if the direct confidences

Table 11: Simulation results obtained with a static topology and time-unvarying confidences with convergent BBAs reached at time $\bar{t} = 5$.

BBA	\emptyset	a	b	c	ab	ac	bc	Ω
$m_1(0)$	-	-	-	0.70	-	-	-	0.30
$m_2(0)$	-	-	-	0.50	-	-	-	0.50
$m_3(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_4(0)$	-	-	0.10	0.30	-	0.15	0.15	0.30
$m_5(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$\bar{m}_1(\bar{t})$	-	-	-	0.70	-	-	-	0.30
$\bar{m}_2(\bar{t})$	-	-	-	0.50	-	-	-	0.50
$\bar{m}_3(\bar{t})$	0.11	-	0.17	0.20	-	0.09	0.09	0.34
$\bar{m}_4(\bar{t})$	0.09	-	0.09	0.27	-	0.14	0.14	0.27
$\bar{m}_5(\bar{t})$	0.11	-	0.18	0.18	-	0.09	0.09	0.35

Table 12: Simulation results obtained with a static topology and time-varying confidences with convergent BBAs reached at time $\bar{t} = 43$.

BBA	\emptyset	a	b	c	ab	ac	bc	Ω
$m_1(0)$	-	-	-	0.70	-	-	-	0.30
$m_2(0)$	-	-	-	0.50	-	-	-	0.50
$m_3(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_4(0)$	-	-	0.10	0.30	-	0.15	0.15	0.30
$m_5(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_2(40)$	-	0.05	0.30	0.10	0.25	0.05	-	0.25
$m_3(40)$	-	-	0.30	0.20	-	0.20	0.10	0.20
$\bar{m}_1(\bar{t})$	-	-	-	0.70	-	-	-	0.30
$\bar{m}_2(\bar{t})$	-	0.05	0.30	0.10	0.25	0.05	-	0.25
$\bar{m}_3(\bar{t})$	0.12	0.05	0.30	0.13	0.05	0.14	0.07	0.14
$\bar{m}_4(\bar{t})$	0.16	0.03	0.13	0.20	0.07	0.10	0.10	0.20
$\bar{m}_5(\bar{t})$	0.12	0.01	0.19	0.16	0.04	0.08	0.08	0.32

change at times $t' < \bar{t}$, the edge selection policy leads the network to reach a different equilibrium point regarding the convergent BBAs.

Table 13: Simulation results obtained with a dynamic topology and time-unvarying confidences with convergent BBAs reached at time $\bar{t} = 31$.

BBA	\emptyset	a	b	c	ab	ac	bc	Ω
$m_1(0)$	-	-	-	0.70	-	-	-	0.30
$m_2(0)$	-	-	-	0.50	-	-	-	0.50
$m_3(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_4(0)$	-	-	0.10	0.30	-	0.15	0.15	0.30
$m_5(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$\bar{m}_1(\bar{t})$	-	-	-	0.70	-	-	-	0.30
$\bar{m}_2(\bar{t})$	0.02	-	0.02	0.48	-	-	-	0.48
$\bar{m}_3(\bar{t})$	0.17	0.02	0.19	0.15	0.09	0.06	0.06	0.26
$\bar{m}_4(\bar{t})$	0.16	0.03	0.13	0.20	0.07	0.10	0.10	0.21
$\bar{m}_5(\bar{t})$	0.13	0.01	0.19	0.16	0.03	0.08	0.08	0.32

4.2.2.2 Dynamic Topology

In this section, we describe the second scenario (dynamic topology) considering the case of both static and dynamic direct confidences for the agents.

Time-unvarying confidences. Consider a dynamic network topology \mathcal{G} where the set of agents \mathcal{V} is static, the set of edges $\mathcal{E}(t)$ can vary over time and the direct confidence produced by the agents does not change over time. In order to consider a dynamic topology, we assume that, at each time step, the set of edges $\mathcal{E}(t)$ may, or may not, contain some of the following edges: $e_{23}, e_{24}, e_{25}, e_{34}, e_{54}$ so that the graph \mathcal{G} is always connected and exhibits at least a rooted spanning tree. For each of these links, we considered a probability of failure $P_f = 0.5$. Table 13 shows the simulation results in terms of convergent BBAs obtained at time $\bar{t} = 31$. The results show that agent v_4 , starts from a probability of normal functioning $P_{m_4}(t = 0) = 0.55$ and reaches a lower probability of normal functioning $P_{m_4}(t = 31) = 0.29$. This can be explained by the occurrence of several link failures that are managed by considering $m_i^f(\cdot)$ as a BBA for the nodes v_i that cannot communicate with node v_j (see section 4.3).

Time-varying confidences. Consider a dynamic network topology \mathcal{G} where the set of agents \mathcal{V} is static, the set of edges $\mathcal{E}(t)$ can vary on time and the direct confidences produced by the agents can also change over time. We assume that, at each time step, the set of edges $\mathcal{E}(t)$ may, or may not, contain some of the following edges: $e_{23}, e_{24}, e_{25}, e_{34}, e_{54}$ so that the graph \mathcal{G} is connected and exhibits at least a rooted spanning tree. Table 14 shows the simulation results in terms

Table 14: Simulation results obtained with a dynamic topology and time-varying confidences with convergent BBAs reached at time $\bar{t} = 50$.

BBA	\emptyset	a	b	c	ab	ac	bc	Ω
$m_1(0)$	-	-	-	0.70	-	-	-	0.30
$m_2(0)$	-	-	-	0.50	-	-	-	0.50
$m_3(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_4(0)$	-	-	0.10	0.30	-	0.15	0.15	0.30
$m_5(0)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_2(5)$	-	-	0.20	0.20	-	0.10	0.10	0.40
$m_3(5)$	-	-	0.10	0.30	-	0.15	0.15	0.30
$\bar{m}_1(\bar{t})$	-	-	-	0.70	-	-	-	0.30
$\bar{m}_2(\bar{t})$	-	0.05	0.30	0.10	0.25	0.05	-	0.25
$\bar{m}_3(\bar{t})$	0.31	0.04	0.24	0.11	0.04	0.11	0.05	0.11
$\bar{m}_4(\bar{t})$	0.16	0.03	0.13	0.21	0.07	0.10	0.10	0.20
$\bar{m}_5(\bar{t})$	0.12	0.01	0.19	0.16	0.04	0.08	0.08	0.32

of convergent BBAs obtained at time $\bar{t} = 50$ and based on a specific set of BBAs obtained by the system of 5 agents through dynamic observations of agents v_2 and v_3 occurring at time $t = 40$. We noticed that the simultaneous change of links and the direct confidences over time leads the network to reach a different equilibrium point.

4.3 CHAPTER SUMMARY

In this Chapter, we presented two data fusion frameworks in the Transferable Belief Model allowing interdependent critical infrastructures to exchange information regarding possible threats and failures in order to increase their situational awareness.

The exchange of information among the infrastructures (based on two different algorithms defined in Denoeux [30]) can be valuable for decision makers during emergency times to understand the most credible cause(s) of infrastructure services degradation, and thus, to take immediate countermeasures. Both algorithms are robust against communication link failures that may occur e.g., due to natural threats.

The outcome of the algorithms can be valuable to take a decision on the occurrence of specific events or threats. To this aim, BetP probabilities can be used to determine if there is "sufficient" information or sensor points so that it is possible to differentiate among the different options.

In Section 4.1, we demonstrated the convergence of the data aggregation algorithm for any connected network topology in finite time

after the last dynamic observations of the infrastructures. We considered a realistic scenario of critical infrastructures equipped with several sensor points that can monitor the occurrence of specific events or threats.

In Section 4.2, we provided simulation results of the data aggregation algorithm defined for any network topology and where the direct confidences of the agents may, or may not, change over time. The framework is suitable to model critical infrastructures which exhibit dependencies with different degree of coupling. We showed how the risk of losing local detail in global decisions because of possible communications failures consists of not being aware of what is experienced by other infrastructures. Anyway, by applying a strategy that increases the credibility of stressed states w.r.t normal states, the speed of the algorithm is preserved.

Both approaches allow to reduce the number of elementary propositions (events and threats) so that it is possible to consider a limited set of states for all considered infrastructures thus decreasing the overall computational time. Anyway, in order to produce an improved global decision, we could enlarge the number of elementary propositions so that they can include information that are specific to "each" infrastructure even at the price of increasing the overall computational time impact required to discriminate the events.

Cyber attacks against supervisory control and data acquisition (SCADA) systems have shown that security violations can compromise the proper functioning of critical infrastructures. The Stuxnet worm [37] exploited vulnerabilities in the information and communications technology layer, ultimately affecting the operation of programmable logic controllers and the uranium hexfluoride centrifuges they controlled. Cyber attacks typically induce faults in sensors and actuators, and alter supervisory mechanisms and notification systems. Once activated, the faults become errors and result in improper operations. These can cause failures in critical infrastructures and eventually affect services, facilities, people and the environment.

SCADA systems are generally unable to cope with cyber attacks primarily because they were not designed with security in mind. Protection from cyber attacks has to be provided by additional security mechanisms that must be integrated with existing SCADA systems in a seamless manner. Logical security is commonly provided by security information and event management (SIEM) systems, which are specifically designed to manage and operate information and communications technology applications.

In this Chapter, we first present in Section 5.2 a methodology to develop a SCADA security testbed [PP14] and also review specific techniques and experiments used to recreate cyber-attacks and explore the possibility of integrating specific simulation models into a SCADA security testbed to assess the impact of cyber-attacks on the physical system.

In the Sections 5.3 and 5.4 we present two platforms that integrate functionalities to assess the impact of cyber attacks based on two network based tools for impact assessment i.e., i2Sim and CISIA respectively (presented in Chapter 3). In particular, in Section 5.3, we report a novel SIEM based platform integrating i2Sim [FDPA⁺14]; whereas

in Section 5.4, we present a SCADA based platform based on CISIA [DPFPP₁₃].

5.1 OVERVIEW

Existing SCADA systems do not employ models and simulations to evaluate real-time the effects of cyber attacks affecting the services produced by interdependent physical systems.

In the following Section, we report the current literature in developing SCADA security testbeds and highlight how the impact assessment functionality is missing in current SCADA implementations. In Sections 5.3 and 5.4, we thus propose two platforms that attempt to integrate this functionality.

5.2 DETAILED REVIEW OF SCADA SECURITY TESTBEDS

In this Section, we review specific SCADA security testbeds taken from the literature and classify the main components of each testbed according to the components identified in the virtual control system environment (VCSE), a SCADA security testbed developed by the Sandia National Lab [58]. This system allows researchers involved in SCADA security to develop and integrate simulation models, emulated device and real physical hardware and to test security policies.

5.2.1 Reference Model

The reference model of a SCADA security testbed consists of interacting software tools and hardware and/or simulated devices that are described in the following and reported in Figure 13:

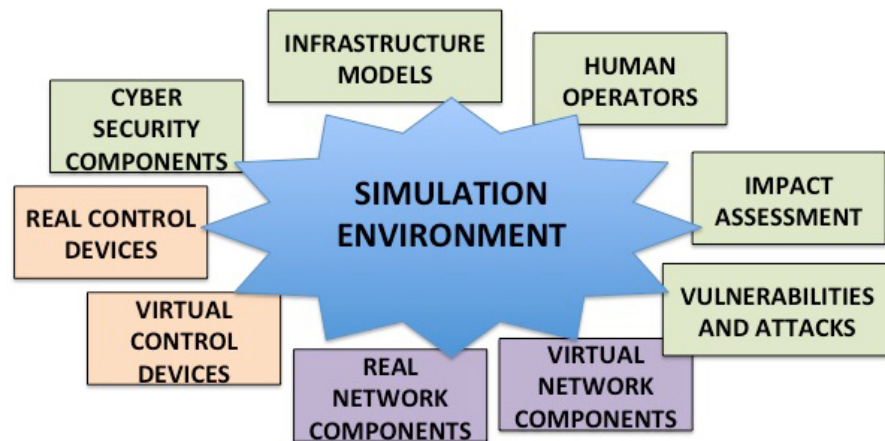


Figure 13: Main components of the reference model of the SCADA security testbed.

1. **Simulation framework:** The simulation framework refers to a software architecture or tool that enables the integration and simulation of different simulation models. It may be based on a discrete event simulation (DES) engine to provide communication among the different components of the architecture.

High-level architecture (HLA) [16] ensures interoperability of models by incorporating simulations on different types of distributed computing platforms as well as supporting reusability of models, as it is possible to use models in different simulation scenarios. OMNET++ [90] is an extensible, modular, component-based simulation framework and offers a set of tools including a graphical runtime environment for the design and implementation of discrete event simulations. It allows the integration of specific modules that can communicate with message passing.

2. **Infrastructure models:** The infrastructure models refer to the models that embed the physical process that is controlled by the SCADA system. Examples include a physical object (e.g., scale model, analogue model, prototype) such as a model used in the wind-tunnel testing to design a new aircraft or a mathematical model (or computer simulation) that simulate the functioning of a power plant.

In the latter case, there exist several commercial or customized software tools (e.g., MATLAB) which allow to build an infrastructure model that provides the functioning of a specific process (e.g., power grid, water plant, Telco system). Computer simulation models may employ a DES engine or exhibit a continuous behaviour presented by a set of differential equations. Such models must be connected to simulated control devices that mimic the functionalities of PLCs/RTUs which in turn receive data produced by simulation executions or send control commands that are translated into changes of the parameters of the model.

3. **Real control devices:** Real control devices consist of remote terminal units (RTU), programmable logic devices (PLC), and intelligent electronic devices (IED) connected to sensors and actuators to implement control actions. They differ from virtual control devices by the fact that they are not simulated. Data collected from the RTUs and PLCs are sent to a human machine interface (HMI) that can make supervisory decisions to change normal RTU or PLC controls.
4. **Virtual control devices:** Virtual control devices are implemented through simulation software tools and may vary according to the configuration features or the emulated functions of the con-

trol devices that they simulate. Commercial software tools emulate the functions of a set of PLCs without the actual hardware. RSLogix family software [32], a PLC simulation tool, allows to configure the hardware of a PLC (e.g., adding modules for CPU, I/O simulator) and to create an emulated PLC simulator that may be integrated into a simulation environment and used to simulate data acquisition from the physical layer or control actions. Once configured, the PLC simulator works as a real PLC. Virtual control devices may also be created by implementing customized software modules able to simulate limited features of a real control devices.

5. Real network components: Real network components refer to communication devices (e.g., routers, switches) that are used to connect the SCADA network (e.g., SCADA servers, HMI, Historian) with the field devices (e.g., RTUs, PLCs).
6. Virtual network components: Virtual network components refer to simulators usually targeted at networking research. Most of them are based on the DES engine and allow to model the behaviour of a network (e.g., a local area network or LAN) by calculating the interaction among components (e.g., hosts, routers, data links, packets). When a virtual network component is used in conjunction with live applications and services, this mechanism is also referred as network emulation.

ns-2 [4] is a discrete event simulator targeted at networking research that provides support for simulation of TCP, routing, and multicast protocols over wired and wireless network.

7. Human operators: Human operators refer to the ability of experimenters to interact with HMIs to monitor and control the proper functioning of the physical process that may be impacted by cyber-attacks experiments on the process itself. A HMI provides different functions including trending information about devices (e.g., sensors), management of procedures, support of expert-systems to handle emergency conditions and it is usually equipped with a mimic diagram to show the status of the system to the operators.

iFIX [8] is a robust SCADA software used to create HMI applications offering usable visualization tools and a reliable control engine.

8. Cyber security components: They refer to novel components able to improve the security of systems. McDonald et al. [58] included open process control system security architecture for interoperable design (OPSAID) [1].

Table 15: Capabilities required for each of the identified categories.

Category	Capability
Simulation framework	- Integration of models (e.g., physical process models). - Providing a graphical interface to design scenarios.
Infrastructure models	Connection with control devices (e.g., PLC) to transfer simulated process data and receive commands.
Real control devices	Performing output results and receiving input conditions within a limited time
Virtual control devices	Simulation of control devices functionalities.
Real network components	Forwarding data packets between computer networks; connection to different data lines from networks.
Virtual network components	- Modeling SCADA components and SCADA specific communication protocols. - Integration with simulation framework.
Human operators	-Visualization on console of physical process data and events. -Performing SCADA actions on the process.
Vulnerabilities and attacks	Implementation of cyber-attacks modeling loss of confidentiality, awareness and control
Impact assessment	Using interdependency model.

9. Vulnerabilities and attacks: Vulnerability and attacks refers to the ability of performing cyber-attacks on SCADA security testbeds by exploiting specific vulnerabilities related to insecure network architectures or operating systems as well as vulnerabilities of wireless devices. Zhu et al. [96] proposed a classification of possible cyber-attacks on SCADA systems, which have a particular focus on the SCADA communication stack using the TCP/IP reference model. Cyber-attacks addressed the network layer (e.g., ARP poisoning, Idle Scan), the transport layer (e.g., SYN flood), the application layer (e.g., Modbus, DNP3), and the implementation of protocols (e.g., TCP/IP, OPC, ICCC).

5.2.2 Comparing SCADA Security Testbeds

In order to present a comparison among specific implementations of the categories presented in previous section, Table 15 reports the main capabilities required for each of the category. Such a list may not be exhaustive because capabilities for each category may from testbed to testbed according to the security objectives that must be demonstrated. Our choice was to consider capabilities that focus most on the possibility of integrating specific categories of components into a simulation environment in order to test the security of a SCADA system.

Genge et al. [43] presented a hybrid architecture where SCADA servers and PLCs are simulated. The control code can run sequentially or in parallel with physical process; in the first case, the framework supports the execution of PLC code remotely including malicious code. However, the study of the effects of cyber-attacks on physical layer has not been analyzed.

Nai Fovino et al. [59] recreated a simulation environment based on real SCADA components allowing the implementation of cyber-attacks through specific malware that are installed on specific SCADA servers that are able to alter the control objectives. Chunlei et al. [21] implemented a testbed based on a software component called SCADA Protocol Tester allowing users to perform flexible implementation of cyber-attacks on a set of SCADA protocols; however no infrastructure model was considered in order to evaluate the consequences of cyber-attacks on the physical process.

Queiroz et al. [70] developed a hybrid architecture where real control devices are integrated into a simulation environment to accept control commands from HMI clients. A DoS was implemented to flood control devices with TCP SYN packets. The limitation of this approach is that the simulation environment does not allow to simulate connection overloads on the control devices that was emulated by limit the number of simultaneous connections at a fixed number.

Chabukswar et al. [18] and Davis et al. [24] implemented a set of DoS attacks that impacted different routers of the simulated SCADA network. However, the two testbeds only use simulated control and network devices.

McDonald et al. [58] implemented a simulation environment based on real control and network devices and performed a set of experiments that are able to alter the control objectives.

Nai Fovino et al. [59] and McDonald et al. [58] seem to be the most relevant testbeds due to the use of real control and network component as well as HMI clients that highlight the real behaviour of the SCADA system against cyber-attacks. In addition, the set of experiments performed are able to alter the control objectives.

An interesting capability that the presented testbeds do not employ is the possibility of integrating interdependency models able to assess the impact of cyber-attacks on SCADA systems and on interdependent technological systems. The two frameworks presented in Sections 5.3 and 5.4 will implement this feature.

5.3 AN I2SIM BASED SCADA SECURITY TESTBED

In this Section, we describe a next-generation security information and event management (SIEM) platform that performs real-time impact assessment of cyber attacks that target monitoring and control systems in interdependent critical infrastructures.

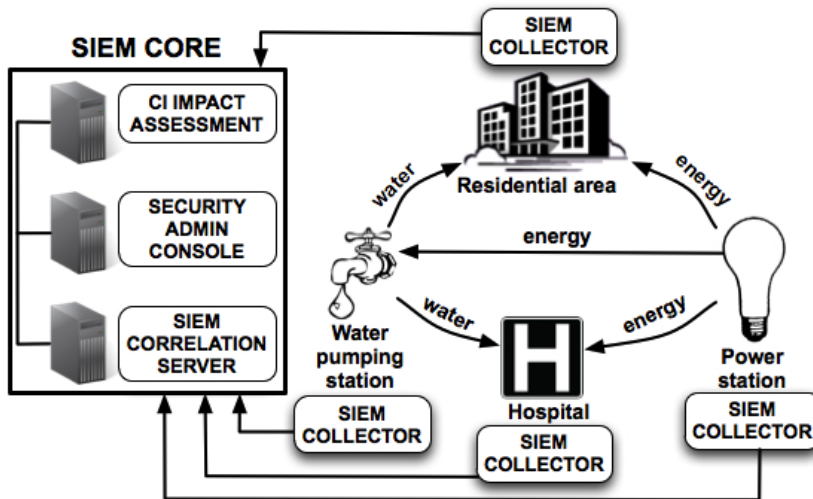


Figure 14: Enhanced SIEM platform architecture.

5.3.1 Software Architecture

Figure 14 shows the architecture of the enhanced SIEM platform. The platform incorporates the following main components:

1. **SIEM Collector:** This component collects data from the monitored infrastructures to provide a multilayer view of system events and cross-correlate data in the proximity of the collection points. The modules responsible for data aggregation are called security probes.
2. **SIEM Correlation Server:** This component correlates events from security probes located in the proximity of critical infrastructure field systems. The SIEM server (based on the OSSIM server) generates high-level alarms when cyber attacks against the monitored critical infrastructures are detected. The alarms contain a risk metric and information about the targeted assets.
3. **Impact Assessment:** This component assesses the impact on the services provided by interdependent critical infrastructures, some of which may be victims of cyber attacks. First, a mapping is performed between the alarms triggered by the SIEM correlation server and the operability levels provided by i2Sim. Next, an i2Sim simulation is executed to assess how the services provided by other critical infrastructures are affected by the new operability levels given the existing interdependencies. The alarms are weighted based on the relevance of the targeted assets to other critical infrastructures. The weighted alarms are sent to human experts or to decision support systems (DSSs) to identify the appropriate countermeasures.

In order to assess the security level of the overall system, the SIEM correlation server operates in a centralized manner. By correlating events and security information, the SIEM server reduces the volume of alerts that reach the higher security event analysis layers thus reducing the number of false positives. Alarm indicators are expressed as numerical values or qualitative indices according to the following impact assessment process:

1. Each event e is normalized by the GET framework in order to have a standard structure and appear as an information vector of the monitored activity $e(x_1, \dots, x_N)$ where N is the number of fields that comprise the normalized event format.
2. The SIEM server stores all the information that can help improve the accuracy of detection by the organization that hosts the SIEM system. This information includes the real vulnerabilities that affect a targeted host (e.g., known bugs) and the relevance of the target as a company asset. This information is referred to as "context information" or simply "the context" and is expressed as a vector of the additional data $a(s_1, \dots, s_m)$. It is worth noting that this information is known only to the organization in charge of the targeted asset, (e.g., a company that manages the infrastructure) because it includes very sensitive information such as hardware characteristics, IP addresses, software versions and business relevance. This information cannot be shared with other infrastructures.
3. The correlation process operates on sequences of events ($e(k)$) and on a vectors. At the end of the correlation process, alarms may be triggered if the security thresholds are exceeded. The SIEM server applies a risk assessment function $R(\cdot)$ to calculate the risk associated with a sequence or pattern of events e in conjunction with the a information, i.e., $R(e, a)$.

For example, consider the implementation of risk assessment as provided by OSSIM SIEM. The OSSIM rules are called directives. When a directive is fired, the following function is applied:

$$\text{Risk} = (\text{Priority} * \text{Reliability} * \text{Asset})/25 \quad (12)$$

Note that the Priority range is zero to five, the Reliability range is zero to ten and the Asset range is zero to five. Thus, Risk ranges from zero to ten. Priority and Asset are assigned through an offline analysis of host vulnerabilities, the typology of the attack and the relevance of the targeted asset to the organization; these constitute the context vector in the model above. Reliability is computed by observing the e sequence and by summing the Reliability of each event. In OSSIM, Reliability is taken to be the probability that an attack is real,

given current events observed in the system. Note that lower Risk values (e.g., zero) are not dangerous because they mean that one of the assessment parameters has very low security relevance.

5.3.1.1 *Metric Transformation*

In order to relate alarms resulting from SIEM analysis to physical modes of each i2Sim cell, the risk assessment value (R) is combined with the service criticality metric (C).

The mixed holistic reductionist (MHR) approach [25] is used to define service criticality. The approach considers interdependency phenomena using three-layers: (i) a holistic layer that considers the evaluation of an event within a critical infrastructure; (ii) a service layer that specifies the services delivered to end users; and (iii) a reductionist layer that models the functional interdependences among different critical infrastructures. The reductionist layer evaluates the impact on a critical infrastructure. i2Sim translates this impact to the impacts on the physical resource flows between multiple infrastructures.

Using the MHR approach, we defined Criticality as the relationships between the attacked nodes (e.g., sensors and actuators) and services (e.g., electric power and water supply). Context embraces the relevance of an asset (e.g., sensor) to the primary infrastructure, namely the relevance of an asset to the business of the infrastructure providing a service. Criticality refers to the relevance of an asset to the infrastructure that uses a service. Thus, criticality is not a unique parameter, but is strictly dependent on the infrastructure that consumes the service; it is computed by the provider based on information shared with the consumer. Indeed, criticality focuses on the need as indicated by the consumer infrastructure, which is not aware of the systems in the provider infrastructure.

5.3.2 *Case Study*

The example scenario uses an attack on the wireless sensor network nodes to demonstrate how the enhanced SIEM system can help evaluate the impact of an attack on infrastructure services. Figure 15 shows the scenario involving a dam that feeds a hydroelectric power station, which feeds a power distribution substation through a transmission network (not modeled for simplicity). Arrows in the figure indicate functional dependencies between critical infrastructures.

The dam provides water to the hydroelectric power station through a gate that is remotely controlled to release basin water and activate the power plant turbine. The dam and hydroelectric power station are controlled by a SCADA system that utilizes a wireless sensor network. Water fed to the hydroelectric power station is conveyed through pipes called penstocks. It is important to guarantee that the water flow values in the penstocks are within the operational range.

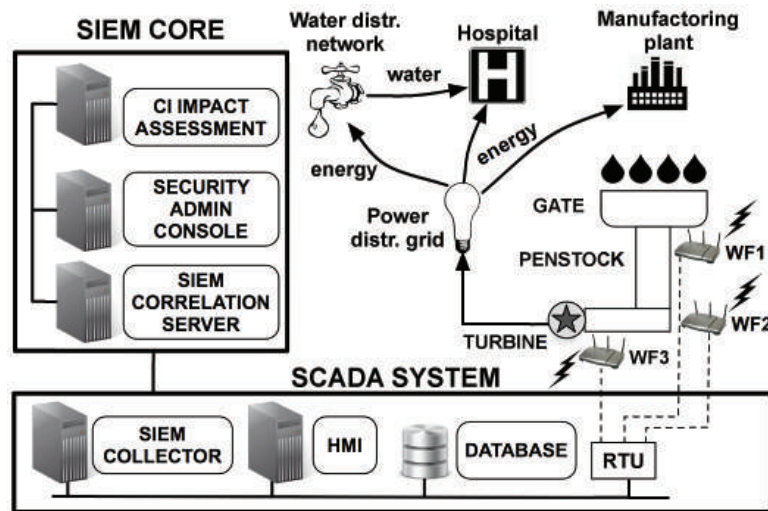


Figure 15: Sample scenario.

Table 16: Electric demands of the CIs considered in the scenario.

Critical Infrastructure	Electric demand (MW)
Hospital	13.47
Water Pumping Station	52.5
Manufacturing plant	9.47

Lower values can result in low power generation while higher values can lead to excessive turbine rotational speeds and turbine vibration, which can result in physical damage to the infrastructure.

A hospital, water distribution station and manufacturing plant receive electricity from the power distribution substation. All the dependencies are modeled using i2Sim. A cyber attack is launched against the wireless sensor network that monitors the dam; the objective is to measure the impact on the operability level of a hospital, which requires electricity and water. Table 16 shows the electrical demands of the critical infrastructures in the scenario.

The wireless sensor network enables the SCADA system to monitor physical parameters. Four types of sensors are used: (i) three water flow sensors placed in the penstocks (WF1, WF2, WF3); (ii) two water level sensors that monitor erosion and piping phenomena under the dam wall (WL1 and WL2); (iii) a tilt sensor placed on the dam gate to measure the gate opening level (inclination); and (iv) a vibration sensor placed on the turbine. The sensors, which correspond to nodes in the wireless sensor network, send their measurements at regular intervals to the wireless sensor network base station (BS). The base station acts as wireless remote terminal unit (RTU) that forwards measurements to the remote SCADA server. Opening commands are issued by the remote SCADA facility to the gate actuator. The in-

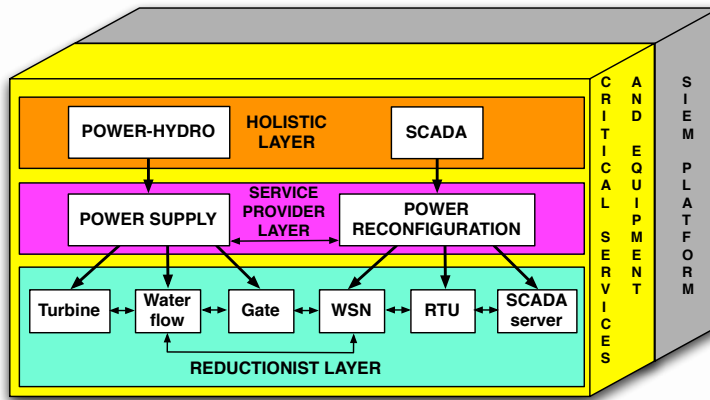


Figure 16: MHR model of the example scenario.

formation and communications technology components deployed include a network-based intrusion detection system (N-IDS) installed in the remote SCADA server facility, a host-based intrusion detection system (H-IDS) positioned in the dam local facility and a SIEM platform with a correlation engine located in a remote office. Figure 16 shows results of the application of the MHR approach and it models the services and equipment that are relevant to the critical infrastructure impact assessment module of the SIEM platform.

Alarms generated by the SIEM correlator are mapped to physical modes of the considered critical infrastructures. Changes to the physical modes of i2Sim result in changes to the resource modes of the affected cells that measure their operability levels.

The scenario considers an attack targeting the wireless sensor network nodes that involves several steps. At the end of the attack, the physical measurements collected by the wireless sensor network nodes are altered to induce incorrect situational awareness about the SCADA system.

The assumption is that the attacker is a dam employee who is allowed to physically access wireless sensor network zones and can connect to the network that hosts the SCADA server, which supervises dam processes.

The attack is performed in two phases. In the first phase, the attacker steals the wireless sensor network cryptographic key. In the second phase, the attacker targets the SCADA server since he can access a host that monitors the dam. Having gained access to the wireless sensor network master node, the attacker reprograms the wireless sensor network nodes. The new program is configured with the cryptographic key obtained during the previous phase. The new malicious code executes the routing protocol by altering the data forwarded from the water flow sensors to the master RTU. Water flow measurement data is altered in order to exceed the control threshold by adding a constant offset to the measured values. In this way, the

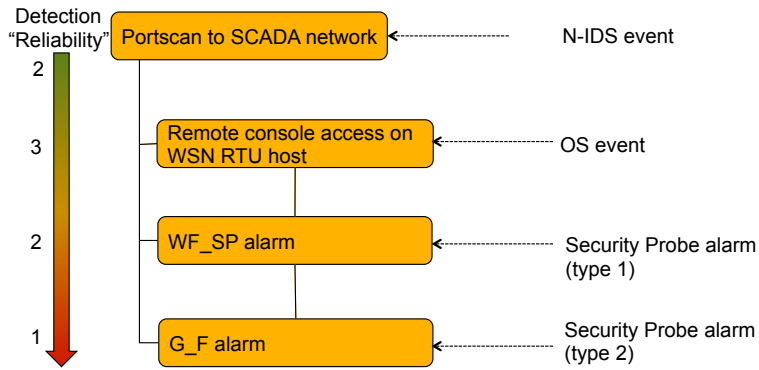


Figure 17: OSSIM rule.

gate is forced to limit water release and ultimately cause low turbine rotation. The final effect of the attack is the reduction in the electricity supplied to the power grid.

In order to detect the attack, we consider events generated by the security probes that oversee the wireless sensors. These security probes detect physical inconsistencies in the sensor data and generate alarms that are processed by the SIEM server: seepage channel sensors should report similar values of water levels; water flow sensors should measure values in the same range; and the gate opening sensor should report a value that is consistent with the water flow in the penstocks. The security probes aggregate the sensor data and verify their consistency.

The anomaly is revealed by two security probes: the first (WF_SP) reveals an inconsistency in the water flows and the second (G_F) reveals a gate opening level inconsistency for all three sensors. Note that another security probe that monitors the water level in the seepage does not show any inconsistency for WL1 and WL2. The alarms from the security probes are correlated by the SIEM platform according to the rule shown in Figure 17.

As indicated in the rule, the Priority is highest (5), Reliability is 8 (sum of single event reliabilities) and Asset has the highest value (5). Thus, the Risk is $(5 * 8 * 5) / 25 = 8$. Considering that the event criticality (C) is in the range 0 to 0.5 (0 is not critical and 0.5 is highly critical) and that the energy production is affected by the wireless sensor network measurements by a factor of 0.5, the resulting impact is $PM = R * C = 8 * 0.5 = 4$. The physical mode (PM) value is the physical mode in i2Sim where a value of one corresponds to fully operational and a values of five corresponds to not operational. Specifically, $PM = 4$ indicates that the cyber attack moves the physical mode functionality down to its lowest energy production level. The 0.5 factor was chosen based on the fact that the wireless sensor network affects the total productivity of the power plant. Figure 7 shows a scenario where a cyber attack against the water flow sensors is de-

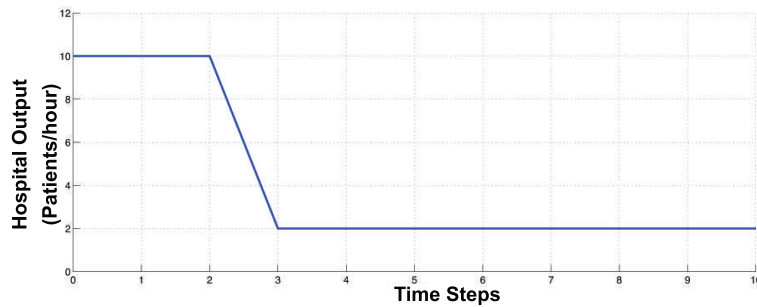


Figure 18: i2Sim results.

tected. Due to the existing interdependency phenomena, the cyber attack degrades the operability level of the hospital.

5.4 A CISIA BASED SCADA SECURITY TESTBED

In this Section, we describe a SCADA security testbed that encompasses infrastructures interdependency models to perform situation assessment. The aim is to enhance the current capabilities of SCADA systems operators with qualitative and/or quantitative measurements of the near future level of risk to reduce the deliberation time and improve the decision outcome in case of faults.

5.4.1 Software Architecture

The network topology of the proposed SCADA security testbed is based on a typical SCADA network architecture which includes Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electrical Devices (IEDs), a Human Machine Interface (HMI) and using a client/server paradigm. Innovative components consist of the Integrated Risk Predictor system (IRP) and a set of Intrusion Detection Systems (IDSs). Both contribute to the impact evaluation of cyber risk associated to the physical components of the SCADA system. The overall network for SCADA security experimentation is distributed over the Internet to emulate the geographic extension of large SCADA systems and consists of three different labs located at the University of Roma Tre and ENEA premises.

Figure 19 shows the topology of the proposed SCADA security testbed. The reference architecture consists of the following components:

- **Process control network:** This network is the connection layer among equipment of the SCADA control centre. A database (DB PCN) stores information about the equipment in the field. Data and information are visualized to operators through a specific HMI. Those information can be retrieved to other operators by

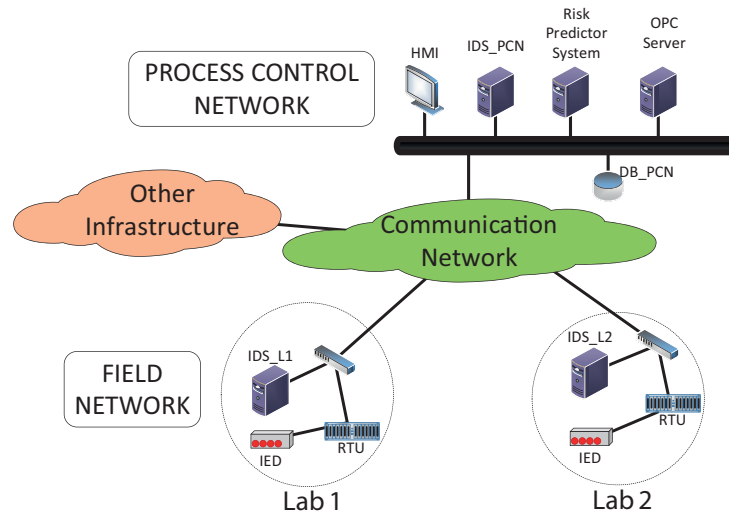


Figure 19: Reference architecture.

means of an OPC (Open Platform Communication) server but also to the IRP which performs a situation assessment by computing the risk level associated to the current state of the considered CI and evaluating the impact of cyber attacks. Cyber attacks can be detected using the IDS associated to the considered CI and related to this network (IDS PCN) whose output is merged into the IRP.

- **Field network:** This network includes sensors, actuators (generally called IEDs) and RTUs and provides the acquisition of process field data and the execution of control actions. In addition, two IDSs (IDS L1, IDS L2), one for each lab, monitor the traffic direct to the RTU, perform a local cyber detection assessment and notify possible malicious activities to the IRP in order to perform a global risk assessment. We assume that an attacker dwells in this network and can implement attacks to compromise the functionality of the SCADA system.
- **Communication network:** This network is the Internet that connects the Process control and Field networks.

Figure 20 presents the modular structure of the IRP. The IRP has six main units: the Mixed-Holistic-Reductionist (MHR), the failure acquisition (F-ACQ) module, the threats acquisition (T-ACQ) module, an OPC client, the Impact visualization (IMP-VIS) interface and the IRP database (DB IRP).

- **OPC client:** The main role of the OPC client is to query real-time data at a fixed time rate from the SCADA database (DB PCN); such data will then be passed to the F-ACQ unit. Data

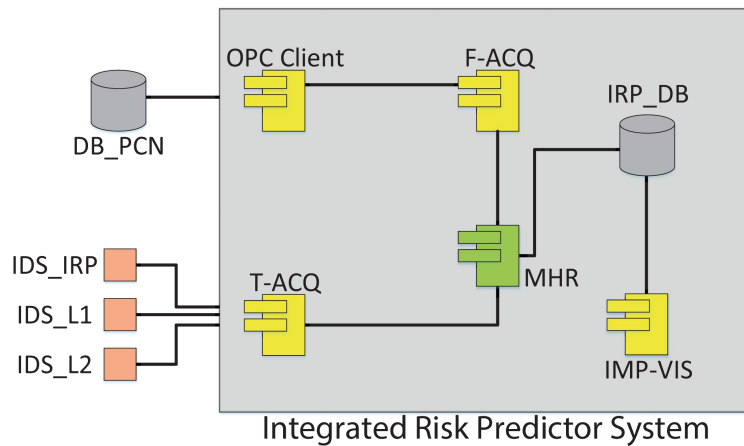


Figure 20: Main components and connections of Integrated Risk Predictor system.

coming from the SCADA system are related to equipment faults and failures, and measurement values.

- Failure acquisition unit:** The main role of this unit is to extract the information relative to the failure occurring on the physical devices from the real-time data provided by the SCADA database. The set of failures occurring on the components and, eventually, the measurement value will then feed the MHR unit to perform real-time impact assessment on the considered CIs. This module can also perform the data translation into an appropriate format compliant with MHR input.
- Threats acquisition unit:** The main role of this unit is to collect real-time data coming from the set of IDSs belonging to the global and local cyber detection assessment. Such data include log information and alert messages that are produced when a malicious attack is detected. Also this module, as in F-ACQ, provides output that is in compliance with MHR inputs. Communications between T-ACQ unit and the IDSs are handled through web service technology: each IDS hosts a web service that accepts requests from web clients hosted in the T-ACQ.
- Mixed Holistic Reductionist model unit:** The main role of this unit is to perform real-time impact of faults and cyber attacks on a set of systems through the execution of an agents-based model. The model represents a network of heterogeneous systems which may exhibit dependencies or interdependencies. MHR model considers CI modelling at different hierarchical levels: Holistic, Reductionist and Service layers. For each CI, agents model the production, supply, transportation (or consumption) of tangible or intangible resources: goods, policies, managements, operative condition, etc. The capability of each

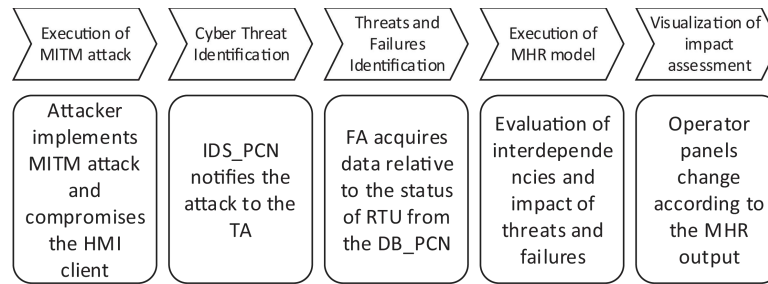


Figure 21: Data workflow for a simple attack scenario.

agent to provide the required resources may depend on its operative condition, which is based on the availability of the resources it requires and on the severity of the failures that affects it. In order to feed the MHR model that generate impact, the F-ACQ and T-ACQ units provide real-time list of failures and malicious attacks.

- **IRP database unit:** The main role of this unit is to store results of the MHR model executions in an appropriate database. This database has been created using MySQL, storing information on the output of the MHR executions. The database includes an historian aiming to maintain all the data for offline analyses.
- **Impact Visualization unit:** The main role of this unit is to provide the operator with a Graphical User Interface (GUI) that shows the real-time and the forecast impact of failures and of attacks to the considered CIs.

5.4.2 Case Study

The case study includes a medium voltage power grid controlled by a SCADA control centre, through a proprietary telecommunication network connecting the control centre with the RTUs. The RTUs are usually modems connected to a set of switches, and they are able to receive and transmit data and information for opening or closing the appropriate switch. Connected to the SCADA network, a general-purpose telecommunication network exists. This network is used in event of far and distant switches or in case of faults, as a backup path.

In the following, we will focus on a specific attack scenario along with the description of the data workflow starting from attack occurrence to attack impact assessment (Figure 21).

5.4.2.1 Execution of MITM Attack

A MITM (Man-In-The-Middle) attack has been performed in our testbed. Referring to Figure 19, the attacker can be located in the Process control network or in one of the two labs connected to the

field devices. The target of this attack is to perform eavesdropping relaying messaging between two different hosts. It is also possible to modify the messages to send fake data to the victim host.

Our implementation of a MITM relies on a known vulnerability of the ARP (Address Resolution Protocol) protocol. The exploit of this vulnerability leads to the ARP-poisoning (spoofing) attack. Our testbed relies on the Modbus/TCP protocol in order to connect the RTU, implemented using a PLC, to the HMI.

5.4.2.2 *Cyber Threats Identification*

The cyber threats identification has been implemented using Snort as an IDS to detect changes in the mapping between valid MAC and IP addresses in order to detect ARP poisoning attacks coming from the SCADA network.

The T-ACQ module acquires data coming from the set of IDSs whereas the F-ACQ unit collects data coming from real equipment e.g. from the HMI. The connection between the T-ACQ and the IDSs is realized via web service technology: each IDS represents the server, and the T-ACQ represents the client that "polls" the servers to gather updated information. The connection between the F-ACQ and the real equipment is realized by means of an OPC client/server architecture. T-ACQ and F-ACQ outputs are related to real equipment and services included into the MHR modelling architecture.

5.4.2.3 *Execution of MHR Model*

The implementation of the interdependency model has been realized using the CISIA tool presented in Chapter 3. Figure 22 shows a representation of such a model containing the relations among the holistic, the service provider, and reductionist layers.

5.4.2.4 *Impact Evaluation*

The impact evaluation of cyber attacks (in our case a MITM attack) on the CIs allows to analyze how attacks can affect equipment and services. MITM attack can have several outcomes. The simple case is collecting information and acquiring knowledge on RTUs, the SCADA system, and their message exchange. In addition, to read requests from HMI to RTUs, attacks can also modify the content of reply messages e.g. in a random way or implementing a "NOT" operator (e.g. in a power grid a circuit breaker command of closure corresponds to an opening command and viceversa). Another possibility is to change the content of packets from RTUs to HMI. In this case, these actions may compromise the functionalities of the SCADA system altering the behaviour of state estimation or control modules.

In both cases, the result of the impact evaluation that is providers to decision makers is given by the estimation of the operative level

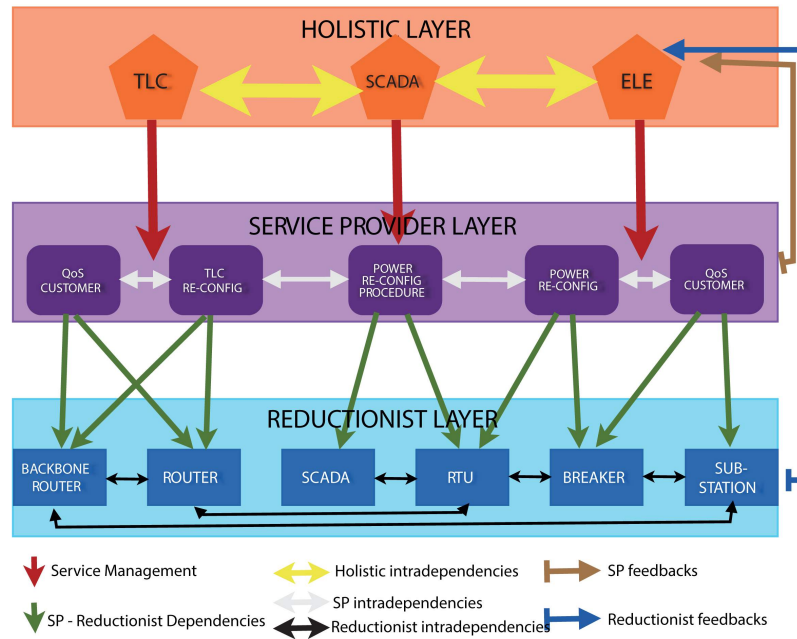


Figure 22: Interdependences model in the MHR approach.

associated to the RTU under-attack and the power reconfiguration service.

5.5 CHAPTER SUMMARY

The technological platforms described in this Chapter are designed to provide the real-time impact assessment of cyber attacks that affect interdependent critical infrastructures. The platforms can detect cyber attacks against wireless sensor network nodes and SCADA components to conduct real-time assessments of the impact of the attacks on the services provided by critical infrastructures.

As demonstrated in the two scenarios, the i2Sim and CISIA models can be used to represent the physical layer and services of an interdependent system in order to analyze the impact of service degradation. The resulting functioning levels can be provided as inputs to an operator dashboard to help make decisions about appropriate mitigation strategies.

Recent years have seen a growing number of critical infrastructures being severely hit by intense hazards manifestations. In 2009, hurricane Sandy brought high winds and coastal flooding in US, leaving nearly 8 million customers without power. In fact, it is well known that floods induced by heavy rainfall can damage the low lines of a power distribution system and cause power disruptions.

In 2013, a 7.1 magnitude earthquake hit the Philippines causing severe damages to infrastructures. When a specific perturbation hit an infrastructure, cascading effects may occur due to systems' dependency, which propagates faults from one system to another.

In this Chapter, we present a Decision Support System (DSS) [RDPL⁺14, BHB⁺14, RPA⁺12] aiming at predicting the possible impact of natural hazards on the services provided by critical infrastructures.

In Section 6.1, we present a brief state of the art on DSS developed within research projects and that can support decision makers during crisis scenarios. In Section 6.2, we present the software architecture of the DSS and its main functionalities. In Section 6.3, we present the impact assessment module of the DSS [TSDP⁺15] that allows to model interdependency phenomena between an electric distribution grid and its SCADA systems and to estimate those substations that may be affected by the loss of tele-control.

6.1 OVERVIEW

Hurricane Kathrina has renewed the interest of the research community and government agencies in developing DSS for supporting emergency planners during crisis scenarios. These complex frameworks allow to predict and visualize real-time cascading effects of multiple infrastructure failures and include disaster support systems

that optimize decision-making during time-sensitive situations. The European UrbanFlood project [6] was aimed at developing an Early Warning System (EWS) for the prediction of flooding in near real time. The system was validated in the context of dike performance in an urban environment and uses sensors monitoring network to assess the condition and likelihood of failures. The system employs flooding specific modules including dike breach evolution and flood-spreading models.

In the context of the European Earth observation program Copernicus, a European Flood Awareness System (EFAS) [7] was developed to produce European overviews on ongoing and forecasted floods to support to the EU Mechanism for Civil Protection. The system is able to predict flood situations more than 3 days in advance based on different weather forecasts interpretation of flood ensemble prediction system forecasts and provides flood alert information.

The Italian national project SIT_MEW [68] has focused on the implementation of an EWS to predict potential impact of seismic events on structures and buildings immediately following an earthquake. The system collects seismic events coming from a seismic monitoring network located in the Irpinia area (Southern Italy) and allows to generate the relative ground motion map from which an expected damage map is generated.

However, existing frameworks do not take into account simultaneously environmental forecasts and (inter)dependency phenomena of critical infrastructures.

6.2 DECISION SUPPORT SYSTEM ARCHITECTURE

In this Section, we present the risk analysis methodology underlying the DSS that is required to produce an estimate of the impact from natural hazards forecasts. Then, we analyze the software architecture of the DSS that implements each step of the risk analysis methodology.

6.2.1 Risk Analysis

In literature, there are several definitions of risk that relate the probability and the intensity of a natural hazard to the physical vulnerability of an element at risk [62]. In order to define the risk in terms of the loss of a service delivered by a critical infrastructure, we provide the following formulation where R_{ij}^x is the risk of loss of the physical component C_i , located in a certain geographical area, belonging to the x -th infrastructure and subjected to the natural hazard T_j :

$$R_{ij}^{(x)} \propto P(T_j)V(C_i^{(x)}, T_j)I(C_i^{(x)}) \quad (13)$$

where:

1. $x \in \{1, \dots, N_{CI}\}$, $i \in \{1, \dots, N_{PC}^x\}$, $j \in \{1, \dots, T_{NH}\}$ with N_{CI} represent the total number of infrastructures, N_{PC}^x the physical components that constitute the x -th infrastructure and T_{NH} the set of natural hazards;
2. $P(T_j)$ is the probability that the natural hazard T_j occurs in a certain area; $V(C_i^{(x)}, T_j)$ is the physical vulnerability (defined as "the degree to which a system is susceptible to, or unable to cope with adverse effects of climate change" [91]) of the i -th component of the x -th infrastructure w.r.t. the natural hazard T_j ;
3. $I(C_i^{(x)})$ measures the effects that the damage of that physical component produces on the system of systems (called *Impact*) and the ultimate effects (called *Consequences*) produced on specific societal criteria due to the loss of the i -th physical component.

We use T_j to indicate a specific threat manifestation (e.g., abundant rainfall, strong wind, lightening etc.) of a given natural hazard (e.g., a tropical typhoon) that constitutes a threat for the infrastructure (e.g., a flooding that may strike on physical components located in flooded areas).

It is worth stressing that eq. (13) should be not meant as an algebraic equation to be solved but rather as a methodological equation stressing which are the terms to be appropriately considered to make a complete risk estimate. In particular:

1. $P(T_j)$ is the probability of occurrence of a specific threat manifestation;
2. $V(C_i^{(x)}, T_j)$ is the probability that a specific element will be damaged;
3. $I(C_i^{(x)})$ whose dimension (either an Impact or a Consequence) provides the ultimate dimension with which the Risk will be evaluated.

From the dimensional point of view, $P(T_j)$ is a probability, the Vulnerability term will be expressed in an arbitrary dimensionless scale (from 1 to 5) while the Impact will be expressed in a dimensionless unit indicating the fraction indicating the reduction with respect to 100%.

Based on the prediction of natural disasters and the detection of seismic events, the DSS is able to produce a **Physical Harms Scenario** (PHS) consisting of a vector containing the set of affected physical components with the associated estimate of the physical damage. The PHS can be generically represented as:

$$\text{PHS} = (\mathbf{c}^\top, \mathbf{d}^\top) \quad (14)$$

where:

- $\mathbf{c}^\top = (C_1^{g_1}, \dots, C_H^{g_H})$ is the set of physical components that are expected to receive an over-threshold probability to be damaged;
- $\mathbf{d}^\top = (D_1^{g_1}, \dots, D_H^{g_H})$ is the set of the extent of estimated damages for each physical component;
- H is the total number of physical components that are supposed to be damaged;
- $g_i \leq N$ indicates the generic infrastructure that may have one or more physical components that exhibit probability to be damaged.

Based on the PHS and the simulation techniques required to propagate the damage of the physical components, the DSS is able to produce an **Impacts Vector** \mathcal{Q} containing the set of the variations of the Quality of Service (QoS) indices associated to each infrastructure. The \mathcal{Q} vector can be generically represented as:

$$\mathcal{Q} = (\Delta Q_1, \dots, \Delta Q_N) \quad (15)$$

where ΔQ_i is the variation of the QoS index of the generic infrastructure i .

In order to measure the consequences for the society, we define a **Consequences Vector** \mathcal{C} containing the results of Consequences estimates in the 4 different criteria [33]: citizens, services, economy and environment.

$$\mathcal{C} = (C_1, C_2, C_3, C_4) \quad (16)$$

6.2.2 Software Architecture

The proposed Decision Support System (DSS) exhibits a four layer architectural pattern used for designing web applications. In the following the four layers are briefly described:

- **Presentation layer:** This layer contains the components that implement the different Graphical User Interfaces (GUI) used by the end users and based on the Geographical Information System (GIS) based framework GeoPlatform. Such GUI include: (i) a GIS advanced interface to visualize GIS maps (e.g., territorial data, seismic maps); (ii) an Impact Reporting Interface to visualise the estimated PHS and \mathcal{Q} vector; (iii) a Consequence Reporting Interface to visualize the predicted \mathcal{C} vector;

- **Service layer:** This layer contains all modules that realize the DSS business logic. In particular, the *Risk Assessment Workflow Manager* orchestrates all the operations required to detect any seismic event occurring in the area monitored by the DSS and produce the relative assessment of impact on the infrastructures;
- **Middleware layer:** This layer implements procedures to gather, on a 24/7 bases, data coming from external sources e.g., meteorological data that are required to feed the impact assessment module w.r.t. natural hazards.
- **Persistence layer:** This layer stores all the data used by the DSS and relative to territorial, census, socio-economic and infrastructure data.

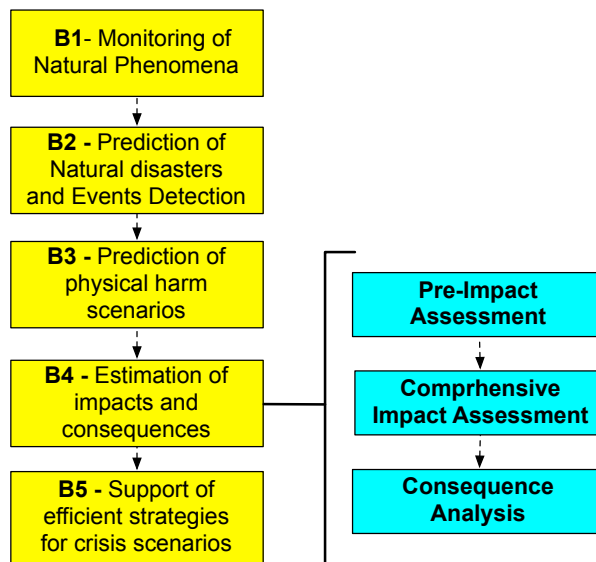


Figure 23: Functional Block Diagram of the Decision Support System.

Figure 23 shows the main functionalities of the DSS in terms of five functional components (Bn):

Monitoring of natural phenomena (B1): This functional block acquires geo-seismic data (i.e., localization and magnitude of seismic events), meteorological forecasts (based on meteorological satellites networks) and nowcasting data (radars in X and C-band). All data have GIS format and represent territorial data, basic cartography, administrative boundaries, road network, hydrography and Census data. Acquisition of seismic data is done on a contours polling at the appropriate Italian National Institute of Geophysics and Volcanology (INGV) [9]; weather forecasts and nowcasting are acquired from official national providers.

Prediction of natural disasters and events detection (B2): This functional block, based on the information acquired periodically from B1, is able to predict, within an estimated temporal horizon, the strength of a limited set of natural phenomena occurring in a specified area.

For each threat manifestation T_j , the system employs specific forecast models to calculate the associated probability of occurrence $P(T_j)$ together with its strength s_j measured with the usual units of measure (e.g., for T_j representing a seismic event, the relative strength measured as a *Peak Ground Acceleration* may be 0.5m/s^2 for a severe event). Further, in order to consider an equal strength scale for all threat manifestations T_j with strength s_j , we defined a specific metric function $F(\cdot)$, called *strength transformation* s.t.

$$F : (s_j) \rightarrow [1, 5] \quad (17)$$

which transforms the effective strength of the hazard into a phenomenological scale containing 5 levels (from 1 to 5). The strength transformation function allows, for each threat manifestation s_j , to define a scale of phenomena manifestation that predict a given environmental situation at a given time t .

Prediction of physical harm scenarios (B3): This functional block evaluates the probability damage that each infrastructure is likely to undergo due to produce the PHS (Figure 24).

Using the transformation function $F(\cdot)$ for all threat's manifestations, it is possible to define a Threat matrix $S(r, t) = S(T_j, F_j)$ that estimates, given a specific location r and a specific time t , the strength of the one (or more) events predicted to occur at that time on that specific location (location where one or more physical components could reside).

Based on a similar reasoning, it is possible to define a Vulnerability matrix $V[C_i(r, t)] = V(T_j, F_j)$ that is a function of the specific element C_i , accounting for the maximum perturbation strength (produced by the different threats) it could sustain before a physical failure.

The physical damage probability $D_{ij}^{(x)}$ to which an element C_i of the x -th infrastructure is submitted by the threat(s) T_j is computed by overlying the two matrices:

$$D_{ij}^{(x)} = \max\{S(T_i, F_j)V(C_i, T_j)\}, \quad (18)$$

When the specific threat T_j manifests with a strength higher than the specific vulnerability threshold $D_{ij}^{(x)}$ of the element C_i , the element will be supposed to fail. The maximum function selects the highest level of failure induced to the C_i by a threat (in the case where many threats simultaneously hit the element).

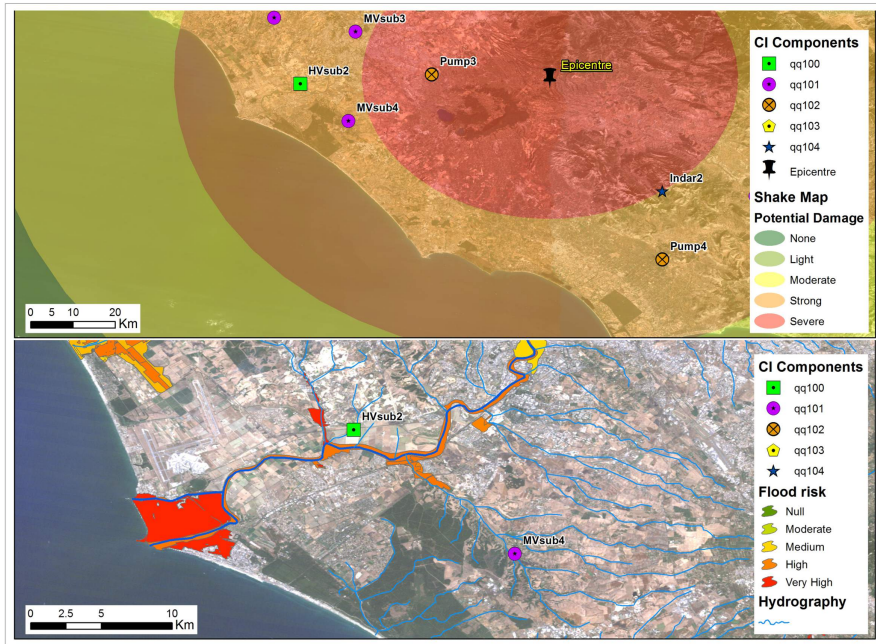


Figure 24: Examples of Physical Harms Scenarios. Upper side: Shake map of a seismic event; Lower side: Flood risk. Each physical component is associated an estimated damage level resulting from the occurrence of the natural hazard (seismic and flooding event respectively).

Thus, if $D_{ij}^{(x)}$ is greater than a specific threshold (e.g., 0.6) then the component is predicted to fail. The set of all $D_{ij}^{(x)}$ not vanishing will constitute the PHS which can be provided to infrastructure operators as alert information.

Estimation of impact and consequences (B4): This functional block estimates the Impacts and Consequences vectors considering services delivered by the infrastructures and the resulting consequences due to the PHS defined in B_3 .

A two-steps process (described in Section 6.3) provides the impact estimation by collecting all the required interdependency information to evaluate the overall impact on all the infrastructures. The consequence estimation is implemented using the predicted impacts and by adopting metrics that evaluate how the loss of infrastructure services may influence a set of social criteria.

Support of efficient strategies for crisis scenarios (B5): This functional block provides crisis managers with a decision list of actions in those cases where the DSS can provide further information required to support a crisis solution.

6.3 IMPACT ASSESSMENT IN ELECTRICAL DISTRIBUTION GRIDS

Electrical Distribution operators use SCADA systems to perform remote or tele-control operations on the electrical grid in order to ensure a constant and efficient energy supply to the consumers. Tele-control operations require a tight interdependency between the Telecommunication and electrical networks: faults in one network produce effects, which in turn reverberate on the other.

Modeling the dynamic of a power network and its dependencies with the other systems such as its SCADA system requires a deep knowledge of the electric network model and this task can be extremely complex using mathematical approaches.

The DSS tackles this issue by using topological properties of the two systems so that, based on the estimated damages on the electric substations provided by the PHS, the system is able to predict within a limited time horizon those substations that can be operated remotely and those that, in turn, would require a manual intervention.

The difference in time of the automatic and manual recovery operations required to reconnect specific electrical loads, is used to predict the outage durations of specific substations and ultimately the consequences for the society.

6.3.1 *Short Time Scale Impact Assessment*

As shown in Figure 23, the impacts evaluation is performed according to a two-step process to take into account the different time scales related to specific interdependencies. In fact, tight coupled infrastructures such as the electrical and the SCADA systems usually activate interdependency mechanisms holding in the short time scale (from a few minutes up to one hour).

When considering other infrastructures, interdependency mechanisms occur with a larger latency. Thus, during very short times scales, other infrastructures could be considered as "decoupled" from the electric and SCADA infrastructures in a sort of adiabatic approximation.

For this reason, the DSS has considered the impact evaluation in two stages:

- **Pre-Impact Assessment:** this procedure analyses the electrical - telecommunication interdependencies to estimate the availability (or unavailability) of electric substations based on the possible occurrences of threats that may alter electric or SCADA components. The outcome of this procedure is the expected outage duration of the electrical distribution substations.

- **Comprehensive Impact Assessment:** this procedure analyses the interdependencies among all infrastructures (e.g., power grid-water distribution, water distribution-hospital) to have a complete assessment of all the domains considered. This procedure takes as an input the expected outage duration of the distribution substations of the considered scenario estimated in the Pre-Impact Assessment module and executes an interdependency model based on i2Sim to evaluate the overall impacts on the infrastructures.

The resulting impacts constitute the \mathcal{Q} vector that is used to estimate the consequences for the society due to the loss of electric supply of specific substations.

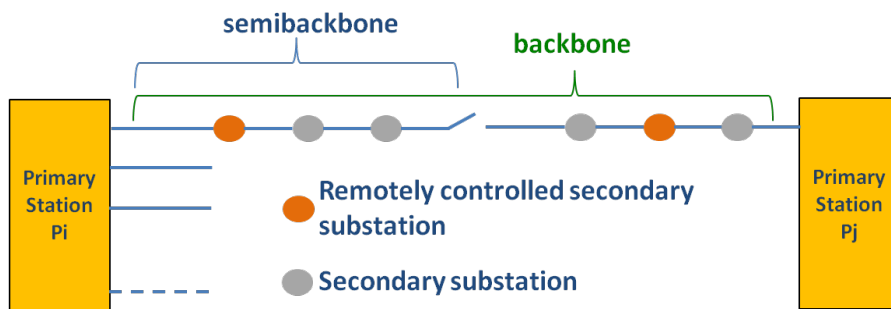


Figure 25: The electrical distribution grid model.

6.3.2 Implementation

Figure 25 shows the considered electrical distribution grid of Rome consisting of a set of High Voltage (HV) Primary Substations (PS) and Medium Voltage (MV) Secondary Substations (SS). Each PS may have one or more Medium Voltage (MV) semi-backbone(s) (SB) ending into other PS. The prefix "semi" is used here to denote that each MV backbone exhibits a normally open switch that decouples the line into two halves where each of them is supplied by one of two overlooking PS. Each SB connects a number of SS where some of them can be remotely controlled.

Each PS has may have on or more backbones that are connected to other PS. The SS are connected in a series configurations and each backbone contains two SB that are divided by a normally open switch that can be closed in order to implement reconfigurations operations. Each SS which is equipped with remote control functionality can be managed by the SCADA control centre serving the electrical distribution grid to implement recovery operations (e.g., to isolate a SS) whereas any generic SS with no remote control functionality cannot be operated remotely. In the latter case, electric operators should send

crewmembers in order to operate on the SS. The remote control functionality serving each SS is provided by a set of Base Transceiver Station (BTS) installed in antennae that are located in the proximity of the SS and that are part of the Mobile Telecommunication network serving the city of Rome.

We assume that the duration of the restoration can last few minutes (about 3-5 minutes) if the SS can be remotely controlled or more (about 50-55 minutes to few hours) depending on several factors (e.g., the time required by emergency crews to reach the faulted substation and to restore it).

Algorithm 3: Reconfiguration procedure.

Data: Electrical and SCADA topology, PHS, SCADA backup times, simulationTime

Result: Electric profiles of substations

```

while time < simulationTime do
    1. Set state of BTS, SS and electrical loads ;
    2. Update remotely controlled SS that cannot receive SCADA
       tele-controls
    3. Update state of each SS
    4. Let time = time + 1
end

```

In Algorithm 3, we present our iterative procedure. The input of the algorithm is given by the electrical grid configuration, the PHS containing damages estimated for the electric and BTS components and time durations parameters for the simulation, BTS backup and the manual restoration of a SS. The output is represented by the electric profile i.e., the amount of unitary energy provided by each SS to its electric consumers during at each time slot.

At step 1) the algorithm sets the state of each BTS, SS and electric consumers supplied by all SS. In particular, each BTS that is predicted to be damaged or that cannot receive power neither from the SS nor by its power backup changes its state from *FUNCTIONING* (if it was working at the previous step) to *FAILURE*. With the same reasoning, each SS that is predicted to be damaged changes its state from *FUNCTIONING* to *FAILURE*. All electrical loads including BTS that are not receiving power from the SS are set to *FAILURE* state.

At step 2), each remotely controlled SS that can no longer receive tele-control from the BTS change its state to *NOT_FUNCTIONING*.

At step 3), the procedure checks if it is possible to restore (i.e., to change its status to *FUNCTIONING* state) all SS that are in the *NOT_FUNCTIONING* state. In addition, the procedure verifies the connectedness of the SS to a PS through manual restoration (if the SS is not remotely controlled or the SS is affected by a damage), auto-

matic restoration from its SB (if the SS is remotely controlled) or from the overlooking SB (by closing the normally open switch).

At step 4), the algorithm increments the simulation time.

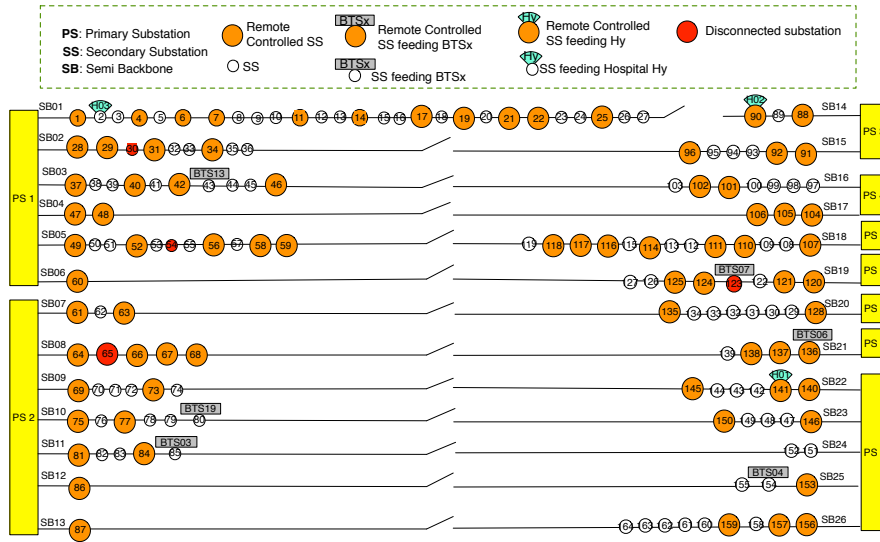


Figure 26: Representation of a section of a power distribution grid of Rome. Rome scenario at time $t = t_0$.

6.3.3 Case Study

In this Section, we consider a real case study given by a section of the power distribution grid of Rome consisting of: (i) 9 HV/MV; (ii) 154 MV/LV SS; (iii) 6 BTS and (iv) 3 hospitals. Each PS has a number of backbones consisting of several SS. Some of these may feed Telecom BTS or hospitals in addition to generic users (e.g., households).

Figure 26 shows the electrical grid at initial time $t = t_0$ and a possible PHS i.e., the set of SS estimated to be in failure (shown in red). Based on our reconfiguration procedure, the Pre-Impact Assessment module estimates the energy profile supplied by each SS over time.

Figure 27 shows the scenario of the electrical grid at time $t = t_2$ with $t_2 = 5$ min. where all the SS that could have been restored through remote control are in a *FUNCTIONING* state whereas others (red ones) are disconnected being in a *FAILURE* state (if considered damaged) or in a *NOT_FUNCTIONING* state if they require manual intervention.

It can be noticed that, at time $t = t_0$, the DSS estimates that 4 substation to be damaged. Then, the algorithm verifies that at time $t = t_1$ (with $t_1 \sim t_0$) the following 33 SS will be automatically disconnected: SS28-SS36, SS49-SS59, SS120-127, SS64-SS68. In fact, being the SS connected in a series configuration, the failure of even *only one* SS in a

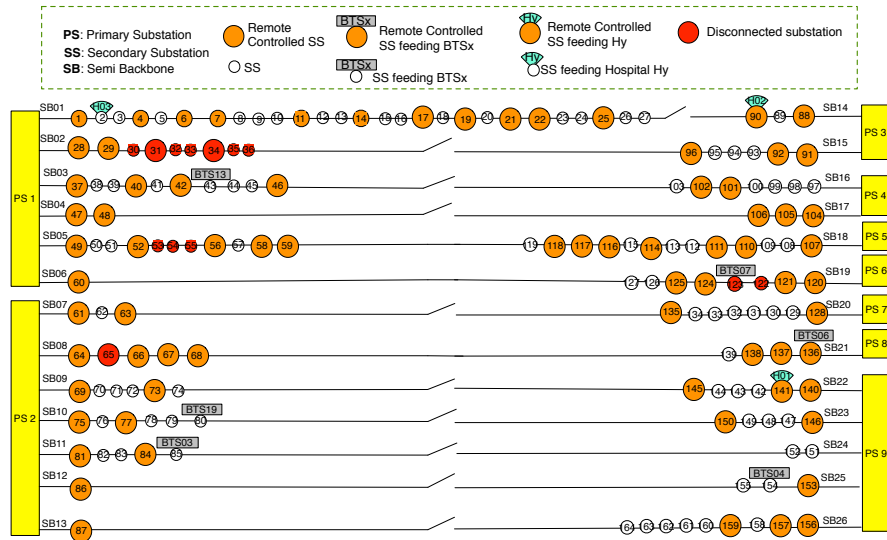


Figure 27: Representation of a section of a power distribution grid of Rome. Rome scenario at time $t = t_2$ (hypothesis: BTS are working properly).

SB produces the opening of all switches at each SS of the SB thus disconnecting all SS.

Considering that some SS can be reconnected through remote operations (in about 5 min.), the algorithm checks those BTS that are in a *FUNCTIONING* state (i.e., that are still receiving power from the secondary substations or that are supplied by electrical backup systems) so that they can be able to send tele-controls to reclose the switches and thus reconnect the disconnected SS. Hence, the algorithm reconnects the following SS: SS64, SS66-SS68, SS49, SS52, SS56, SS58, SS59, SS120, SS121, SS124, SS125, SS56, SS58, SS59, SS116-SS118, SS114, SS110, SS111, SS107, SS28 and SS29.

At time $t = t_2$, the algorithm verifies that the failure of SS123 that feeds BTS07, which, in turn provides remote control to the SS96, has the effect that the SB02 cannot be connected (through the closure of the switch located in SS96) to SS36, thus leaving several SS in SB02 in a *NOT_FUNCTIONING* state.

This behavior is shown in Figure 28 where 12 substations cannot be reconnected through remote control (SS30-SS36, SS53-SS55, SS122, SS123, SS65). The figure also shows that, without the dependency information among the SS and the BTS, the decision makers (e.g., an electric operator) receiving only the information of the possible damaged substations may not be able to infer that "additional" SS could be affected due to the failure of the BTS.

In addition, the information provided could also be used to plan an effective intervention of crewmen that can be sent to the affected

SS in a sequence that minimizes the overall number of the affected SS or the number of affected electric consumers.

The expected outage duration of the SS feeds the Comprehensive Impact Assessment module based on i2Sim that subsequently evaluates the Impacts Vector \mathcal{Q} i.e., the resulting impacts on the other infrastructures present in the scenario. The \mathcal{Q} vector together with census data may feed specific metrics able to estimate the Consequences Vector \mathcal{C} .

These information may be useful for decision makers to know, during crisis scenarios that in a specific area there might be a high concentration of citizens (e.g., old aged people, disabled people) that may be severely affected by the different outages of primary services (e.g., water, gas) resulting as cascading effects of the unavailability of electric power. These aspects will be investigated in Chapter 7.

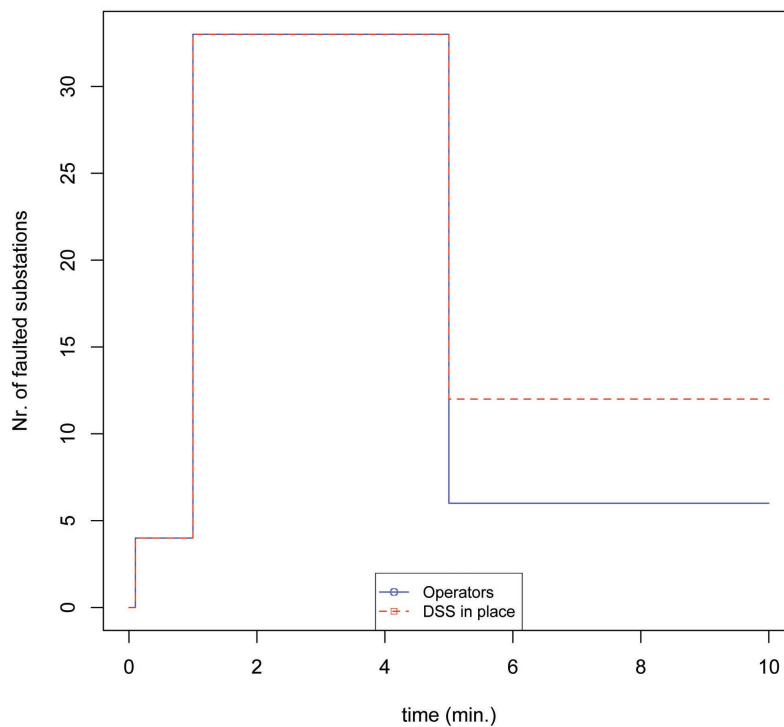


Figure 28: Profile of the estimated substations in failure state.

6.4 CHAPTER SUMMARY

In this Chapter, we attempt to solve the full risk analysis workflow, from events prediction to impacts and consequences estimation of a critical scenario.

The Decision Support System presented in Section 6.2 uses Geographical Information System (GIS) technology to map the prediction

of natural phenomena or the magnitude and localization of seismic events to the possible impact on critical infrastructures.

In Section 6.3, we described a core component of the DSS i.e., the Pre-Impact Assessment module allowing to estimate the possible effects of specific natural threats to the electrical infrastructure. Indeed, the reduction of the quality of services of the electrical infrastructure may produce negative effects on all human activities and the societal life in general. This module constitutes the bases to implement a Comprehensive Impact and Consequences Assessment module.

RESOURCES ALLOCATION IN EMERGENCY SCENARIOS

Recent events, such as Hurricane Katrina, have revealed the need for coordinated and effective disaster responses. An optimal distribution of available resources such as electricity and water is essential for disaster response effectiveness.

The ideal would be to deploy unlimited resources to protect large urban areas. However, during emergency times, in practice service resources are often limited. Thus, the problem faced by emergency responders becomes how to allocate limited resources in order to minimize the negative impact on the delivery of critical services and preserve the security of citizens.

In this Chapter, we present different approaches aiming to suggest to decision makers mitigation actions, which minimize the negative impact of failures affecting dependent critical infrastructures.

The Chapter is organised as follows: Section 7.2 presents two approaches based on genetic algorithms to define the optimal allocation of resources that maximise the delivery of infrastructure services [DPLP⁺15], [RDPL⁺14]; in Sections 7.3 and 7.4, in order to maximize the operability of an hospital, two approaches based on Ordinal Optimization [AADP⁺14] and simulation [55] respectively, are presented.

7.1 OVERVIEW

In literature, different approaches have been studied to improve response readiness of emergency transportation facilities such as fire engines, fire trucks, and ambulances during crisis. This problem belongs to the general category of facility location, whose formulations and solution algorithms have been discussed by Farahani et al. [95]. These approaches include the application of a covering model that maximizes the coverage of demands, given acceptable service distance/time, when limited resources are available.

Other approaches focus on optimizing allocation of available resources according to the type disaster such as wildfires [66], earthquake [38], and public health emergencies [12]. Different approaches have been developed to model the disaster scenarios including: mathematical formulation [39], and stochastic simulation model [66].

In this Chapter, we employ procedures and existing physical domain simulators to form a simulation-based environment for acquiring/modeling disaster events. Then, we develop different techniques to find the optimum allocation of available resources.

7.2 GENETIC ALGORITHMS BASED APPROACHES

In this Section, we define two approaches providing optimal resources allocation for a power distribution network that delivers energy to a set of infrastructures and domestic users.

The power distribution network is subjected to possible physical failures that may disconnect substations and this may impact the functionality of dependent infrastructures. In cases of outages, a decision should be taken by electric operators or decision makers (e.g., civil protection operators) to maximize both the power delivery to the loads and the level of services provided by the infrastructures as well as to minimize the consequences for the society.

In order to leverage the computational time required to calculate the goodness of each resource allocation, we use Genetic Algorithms (GA) which were introduced by Holland in 1975 [48]. GA work iteratively with populations of candidate solutions in order to determine the set of individuals that are considered possible optimal solutions to a problem. GA are based on the process of natural evolution to find individual solutions which can prevail over those that are less strong at each generation. To this aim, the fitness of every individual solution is evaluated using criteria that are application-dependent. Then, the solutions with higher fitness values are selected (with higher probability) to form the population of the next generation. GA use crossover and mutation operations to choose the individuals of the next population and alter them to increase fitness as generations progress.

7.2.1 *Load Shedding Problem*

The optimization procedure consists of the following steps:

1. Execution of the load flow calculation to verify that the network is still able to supply the nominal power to the loads after the failure of some physical components;
2. Application of a load shedding algorithm to emulate a possible electrical operator action aiming at leveraging the affected network;
3. Execution of the izsim model initialized with the electrical load values calculated in 2).

This problem may be formally defined as follows:

$$\begin{aligned}
& \underset{L}{\text{maximize}} && Z(t) = Q^e(t, L, W^e) + Q^u(t, L, W^u) \\
& \text{subject to} && 0 \leq l_i \leq P_i \quad i = 1, \dots, N, w_i^e \geq 0, \quad i = 1, \dots, N; w_i^u \geq 0, \quad i = 1, \dots, K \\
& && \sum_{i=1}^N w_i^e = 1, \sum_{i=1}^K w_i^u = 1, W^e = \{w_1^e, \dots, w_N^e\}, W^u = \{w_1^u, \dots, w_K^u\}
\end{aligned} \tag{19}$$

$$Q^e(t, L, W^e) = 1 - \frac{\sum_{i=1}^N (1 - w_i^e)(P_i - l_i)}{\sum_{i=1}^N P_i} \in [0, 1] \tag{20}$$

$$Q^u(t, L, W^u) = \frac{\sum_{i=1}^K w_i^u Q_i^u(t, L, W^u)}{\sum_{i=1}^K S_i} \in [0, 1] \tag{21}$$

where:

- l_i is the active (reactive) power demand value in MW (VA) of load i at time t ;
- W^e and W^u are weight vectors needed to prioritize specific loads and services;
- $Q^e(t, L, W^e)$ represents a QoS index of the electrical network and reaches the maximum when all the loads l_i are consuming the expected power value P_i ;
- $Q^u(t, L, W^u)$ represents a QoS index of the services provided by the infrastructures that depend on the loads supplied and on the interdependencies phenomena and reaches the maximum when all infrastructures are providing the nominal service level S_i .

Hence, by maximizing $Z(t)$, we are choosing the combination of electrical load values that maximize both the power supply to the loads and the service delivery of all infrastructures which, in turn, depend on the energy supply of those loads (e.g., water and gas distribution, health services).

In particular, in order to calculate the $Q^e(t, L, W^e)$, we use the electrical simulator PSS Sincal [5] to execute the load flow calculation and verify the feasibility of the load shedding configuration and use izsim to calculate $Q^u(t, L, W^u)$.

A possible formulation of $Q_i^u(t, L, W^u)$ for a hospital is a linear function that relates the number of patients healed per hour to the availability of specific services (e.g., equipment, operation theatre) that, in turn, depend on power supply.

It is worth stressing that, when applying this procedure to a real scenario, the choice of W^e and W^u poses an ethic issue since their values influence which loads and services will be prioritized.

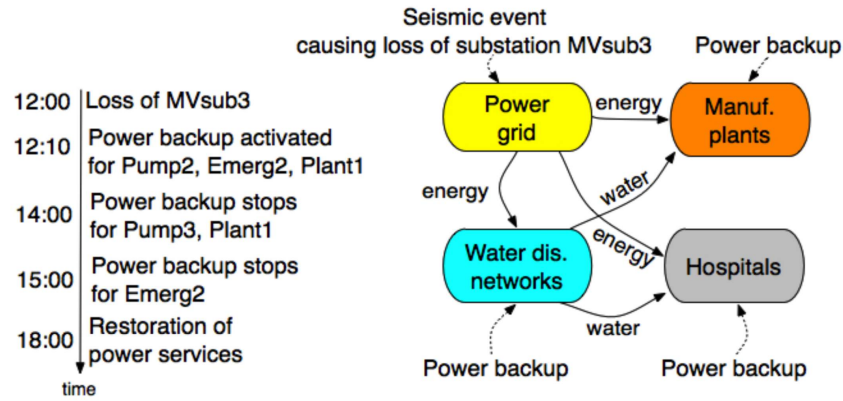


Figure 29: Sample scenario: functional dependencies involving a power grid, water distribution networks, hospitals and manufacturing plants.

7.2.1.1 Case Study

Let us consider a scenario given by a set of dependent infrastructures affected by a seismic event. Figures 32 and 31 show the scenario consisting of the following infrastructures:

- Three power plants that supply energy to a high voltage (HV) 150 kV power transmission grid connected to three medium voltage (MV) 15 kV power distribution grids;
- Three water distribution networks;
- Three hospitals;
- Three manufacturing plants.

By an electrical point of view, we considered the loads as aggregated loads (e.g., Plant1 consists of different plants).

At a functional dependency level, the MV power distribution grid supplies energy to the water pumping stations, to the hospitals and to the plants, whereas the water pumping stations supply water to the hospitals and the manufacturing plants.

We assume that:

- The seismic event occurring at 12 a.m. and affects a MV electrical substation (MVsub3) with the consequence that it is unable to satisfy the average electrical demand (Table 17).
- The trend of the water and energy demand for the loads remain constant in time;
- The procedure takes the damage scenario i.e., the list of estimated failed physical components as an input.

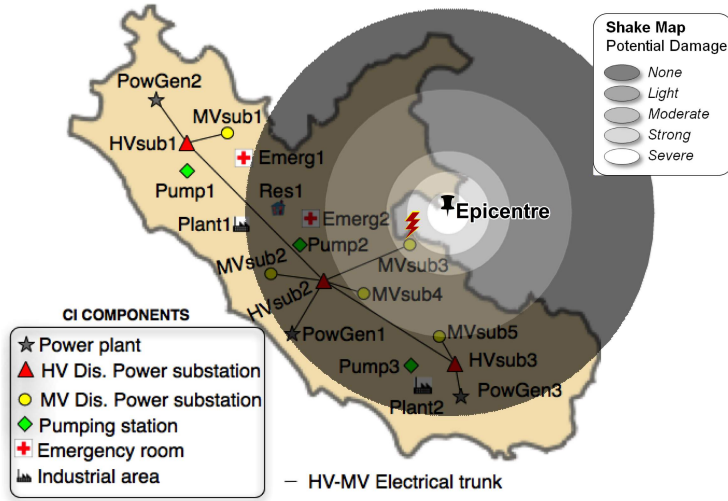


Figure 30: Sample scenario: geographic representation the shake map relative to the seismic event. The lightning indicates the physical components that are estimated to be damaged due to the occurrence of the seismic event.

Table 17: Electrical Power balance (active power, MW) resulting from the load shedding actions in case I and II.

Time	Case	MVs2	MVs3	MVs4	Pump2	Res1	Emerg2	Plant1
12:00	-	15	6.5	11.5	1	15	2	10.5
12:10	I	7	0	9.5	0.5	8	2	7
12:10	II	7	0	10	1	7.5	2	7

Regarding the latter, we can consider that a seismic sensor network located on the field acquires the epicentre and magnitude values of the seismic event occurring in the considered scenario. Then, such information can be combined following an approach similar to that presented in Chapter 6 to evaluate the damage scenario. In particular, starting from the severity of the seismic event and considering the physical vulnerability of the substations buildings to seismic events, the set of substations that can be affected by earthquakes can be found and used as an input by our procedure.

For the sake of simplicity, we limit our impact assessment analysis to services provided by Res1, Emerg2, Pump2, and Plant1.

In the following, we describe an application of our procedure to the considered scenario and show how it can provide a valuable support to decision makers. To this regard, we compare the case where the electric operator takes decisions only by applying its mitigation plans (that usually do not consider interdependency phenomena) with the case where the operator, through our procedure, tries to maximize both the power supply to the loads and the service delivery of all infrastructures.

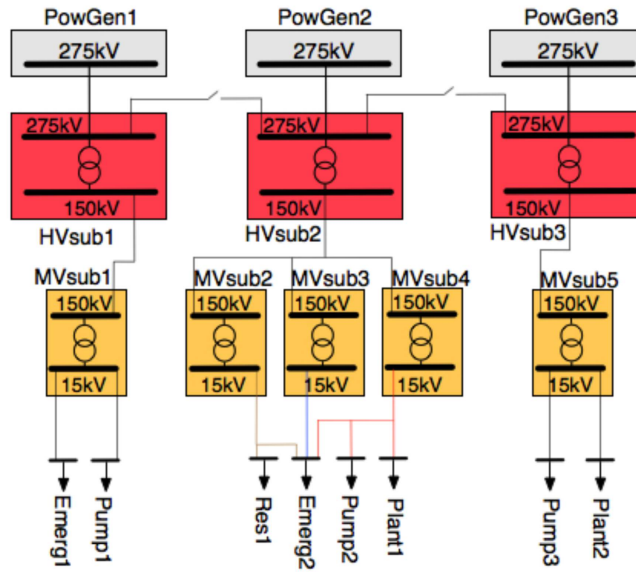


Figure 31: Power grid model. Grey boxes: power generators; red boxes: High Voltage substations; yellow boxes: Medium Voltage substations; arrow: electrical loads.

Table 18: Critical Infrastructure Service Layer (Case I and II).

Time	Water (Kl/h)		Patients per hour		Pieces per hour	
	Case I	Case II	Case I	Case II	Case I	Case II
12:00	375	375	4	4	4.5	4.5
12:10	281	375	3.9	4	3	3
14:00	187	375	2	4	1.5	1.5
18:00	375	375	4	4	4.5	4.5

Case I: Starting from the damage scenario, the electrical operator might perform actions to counteract the perturbed conditions following the physical damage to MVsub₃ substation.

Its actions will be reasonably based on contingency plans and/or simulations that predict the new state of the network in order to maximize the power supplied to the loads, particularly to the critical ones (e.g., Emerg₂). Considering that the electrical operator will try to maximize its own network and that, in general, it is not aware of all the (inter)dependency phenomena among the infrastructures in the considered area, its actions might not contribute to increase the service level of specific infrastructures.

For instance, a possible load shedding action that supplies the expected power demand to Emerg₂ and that isolates some water pumping stations aggregated into Pump₂ (e.g., by supplying 0.5 MW instead of the expected power demand i.e. 1 MW) might have the consequence that Emerg₂ is not receiving the ex-

pected water demand. The further consequence would be that the performance of the emergency room (which requires water to work) will be deteriorated thus reducing the average number of patients healed per hour. Table 17 shows a possible network configuration following a load shedding action that supplies the expected power demand to Emerg2 and isolates some water pumping stations. Table 18 shows the resulting infrastructure service level estimated by an appropriate i2sim model that is delivered to the decision makers. It should be noted that the modeling of the power backup systems (active during the interval 12:10-15:00, see fig. 2) for Pump2, Emerg2 and Plant1 in the interdependency model allows to maintain a minimum infrastructure service level until the functioning of MVsub3 is restored (at 18:00).

Case II: In this case, the presented optimization procedure is applied to maximizing both the power supply to the loads of the power grid (where substation MVsub3 is out of service) and the service delivery of the infrastructures.

In the following, we define the parameters of an instance of the considered optimization problem for our scenario:

$$\begin{aligned} w_{\text{Emerg2}}^e &= 0.5; w_{\text{Pump2}}^e = 0.2; w_{\text{Res1}}^e = 0.2; w_{\text{Plant1}}^e = 0.1; \\ w_{\text{Emerg2}}^u &= 0.5; w_{\text{Pump2}}^u = 0.3; w_{\text{Plant1}}^u = 0.2; P_{\text{Emerg2}} = 2; \\ &P_{\text{Pump2}} = 1; P_{\text{Res1}} = 15; P_{\text{Plant1}} = 15; \end{aligned} \quad (22)$$

where the power hospital supply and its service delivery are prioritized. In general, the optimization problem (19) may be solved using different techniques. For our sample scenario, given its simplicity, we were able to enumerate all possible solutions and to select the optimal one. Table 17 reports the optimal solution where some of the electrical loads aggregated into Pump2, Res1 and Plant1 nodes were disconnected as a consequence of the computed load shedding action.

Respect to case I, the possibility of considering also the existing interdependency phenomena, it allows to increase (in time) the average patients treated rate of Emerg2 (due to the nominal functioning of the water pumping stations of Pump2) that is considered of primary importance (see 18).

Anyway, in general, the mere enumeration of all the possible solutions it is not possible. In the following, a possible Genetic Algorithm (GA) problem solution is presented to describe the challenges that should be faced within the DSS implementation. The proposed GA provides the best electrical network configuration that maximizes the objective function in (19). The simple

GA scheme described in this work does not consider the network reconfiguration operation as well as the possible activation of distributed power generation facilities.

Algorithm 4: A GA for the load shedding problem

```

Data: IPS: the Initial Population Set
Result: Best Available Load Shedding Configuration
/* PS denotes the Population Set */
PS ← IPS;
repeat
  /* Evaluate the Fitness Value of each chromosome in
  the PopulationSet */
  for i = 0 to |PS| do
    | EvaluateFitness (Chri)
  end
  PS ← CrossOver (PS);
  mutation ← CheckMutationNeeded;
  if mutation then
    | PS ← Mutation (PS);
  end
  /* The algorithm uses Stall generations stopping
  criteria */
until stop;

```

In the proposed GA scheme, each *chromosome* represents a load shedding configuration through a vector of real values *genes* of length N where N is the number of loads in the proposed electrical network (i.e., a *chromosome* is a potential solution of the optimization problem).

The real value of each gene represents the active power assigned by the load shedding configuration in the specific chromosome. For instance, the chromosome (2.0, 1.0, 15.0, 1.0, 2.0, 15.0, 1.0, 12.0) represents a specific active power assignment to the *Emerg1*, *Pump1*, *Res1*, *Pump2*, *Emerg2*, *Plant1*, *Pump3*, *Plant2* loads of Figure 31 respectively. We supposed that, if an assignment of active power to a load defines a specific decrease factor w.r.t to the nominal active power, the same decrease factor will be applied to the load reactive power value.

In addition, a load shedding configuration represented by a particular chromosome is considered admissible if the constraints are satisfied and the resulting electrical network configuration is valid (i.e., load flow convergent, no lines overloaded).

The described algorithm poses new challenges w.r.t to classical GA implementations (e.g., fine tuning of the classical GA parameters) [54]. In order to leverage algorithm from the computational point of view, different strategies may be applied: (i)

execute the algorithm with an initial population containing *good* solutions; (ii) remove from the problem the critical loads that should not be disconnected; (iii) execute the algorithm with pre-calculated izsim runs; (iv) include in the problem the electrical constraints to avoid calling the power simulator; (v) parallelize the problem.

The sample scenario shows how the optimization procedure may be able to suggest mitigation actions to decision makers that would not be considered by common contingency plans of CI.

7.2.2 Crewmen Optimization Problem

In this Section, we present an application of the reconfiguration algorithm for Electrical Distribution Grids developed inside the DSS presented in Chapter 6 in order to show how it is possible to minimize the negative consequences for citizens due to the degradation of infrastructure services.

In particular, we suppose to have a limited number of emergency teams available by the Electric Distribution Grid which aim is to implement manual interventions on the Secondary Substations (SS) that are predicted to be damaged by the Physical Harms Scenario (PHS) (provided by the DSS B₃) or that are disconnected due the unavailability of remote tele-control.

The optimization stands on how to distribute the emergency teams considering that they are limited in order to reduce the Consequence for the society.

7.2.2.1 Wealth Indices

In order to measure the consequences for the society due to the loss of infrastructure services, we introduce the concept of *Wealth* that, in general, encompasses a large number of issues e.g., economical, related to societal health and to other domains defining the GPI (Genuine Progress Indicators).

In particular, we focus on the definition of a subclass of Wealth indices, which are related to the outcomes of the access and the availability to primary and vital technological services. The access to these services brings a number of beneficial consequences, which we wish to appropriately measure. With such indicators, we are able to measure the reduction of well-being (Wealth) consequent to Services unavailability.

Let us define the Wealth $W(t_{ij})$ of a Consequence Criterion element t_{ij} as a function of the available Services Q_k as follows:

$$W(t_{ij}) = M(t_{ij}) \sum_{k=1}^{N_k} r_k(t_{ij}) Q_k \quad (23)$$

Table 19: Considered Consequence Criteria.

Consequence Criterium	Electricity Service
Aged people t_{11}	$r_1(t_{11})$
Children t_{12}	$r_1(t_{12})$
Disabled t_{13}	$r_1(t_{13})$
Average citizens t_{14}	$r_1(t_{14})$

where:

- N_k is the total number of the considered services which contribute to wealth;
- M is the metric for wealth measure. This could be related, for instance, to GDP produced per hour of activity (for a firm), or the number of patients healed in a unit of time for an hospital or the extent of land which might efficiently be used for some industrial or environmental purpose etc.
- $r_k(t_{ij})$ is the relevance of the k -th service for the achievement of the maximum level of the wealth quantity M for a given element of riterium t_{ij} (Table 19). It might happen that a specific service, more than others, enables the achievement of Wealth (e.g., electricity for people depending on biomedical devices, water availability for specific plants) and other being less vulnerable for a lack of it;
- Q_k is the variation of QoS of the generic infrastructure k .

To evaluate the consequence C on the consequence criterion element t_{ij} due to the Q_k variations (in time), we integrate, on the time duration T of the Crisis, the following expression (assuming $r_k(t_{ij})$ is independent on time):

$$C = M[1 - \sum_{k=1}^{N_k} r_k(t_{ij}) \int_0^T Q_k(t) dt] \quad (24)$$

where:

- W_0 is be the total Wealth during time T without the perturbation;
- the second term at the r.h.s. represents the effective wealth of the consequence criterion element due to the crisis, i.e., due to the variation in time of the QoS of one or more services.

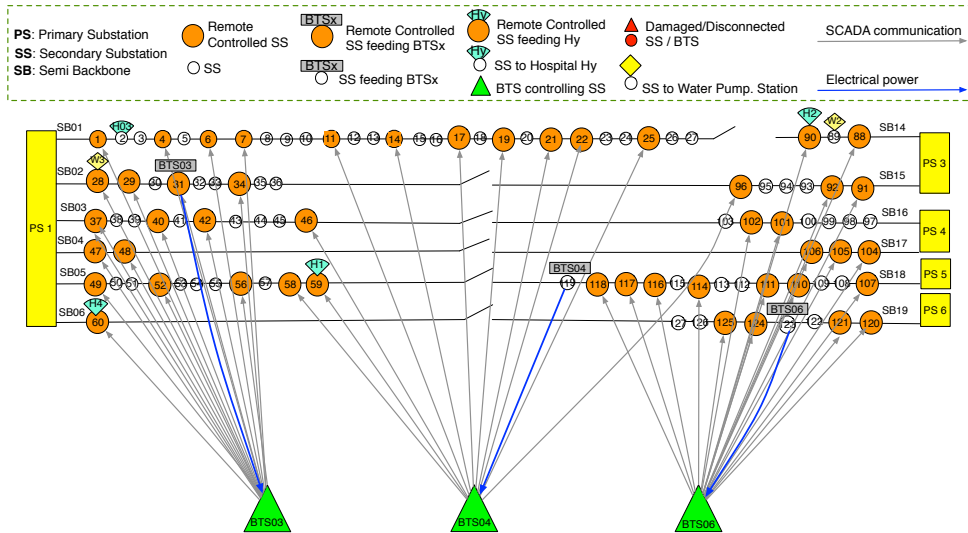


Figure 32: Case study: representation of a section of the electrical distribution grid of Rome. Arrows indicate the interdependency among Electrical and SCADA systems.

7.2.2.2 Case Study

As a case study, let us consider the section of the electrical grid of Rome shown in Figure 32. Let us consider the following assumptions:

- $M = 100$ is the total number of SS including those that allow tele-control;
- The network can be affected by F damages at specific SS that are given by a generic PHS at a certain time.
- The electrical operator can only have R emergency teams to implement the N manual interventions that include the F damaged SS and the $N - F$ SS that cannot work due to the unavailability of remote tele-control.
- The generic emergency team m for $m = 1, \dots, R$, with R being the total number of emergency teams available to the electric operator, should operate a manual intervention to a set of SS according to an ordered sequence of interventions $\{S_m\} = \{SS_m^1(\Delta T_m^1), SS_m^2(\Delta T_m^2), \dots, SS_m^N(\Delta T_m^N)\}$ with the generic J_k s.t. $0 \leq J_k \leq N$ and ΔT_m^k being the time required to reach the faulted SS (that depends on the distance and the predicted traffic road conditions) and to implement the manual intervention (that can be considered fixed).

Our resource optimization procedure, is applied to find a (sub)-optimal allocation of resources to the problem of minimizing the consequences. The solution of this problem would be represented by a

sequence of interventions $\{S\}$ enabling the complete restoration of the system, with the requirement of producing the smallest possible consequences for the considered criteria.

It is easy to understand that different restoration sequences could produce different consequences: some sequences could be preparatory for other restoration and/or enabling some actions to be performed more rapidly.

In general terms, the optimal solution $\{S_m\}$ will be:

$$\{S_m\} : C \text{ is minimum} \tag{25}$$

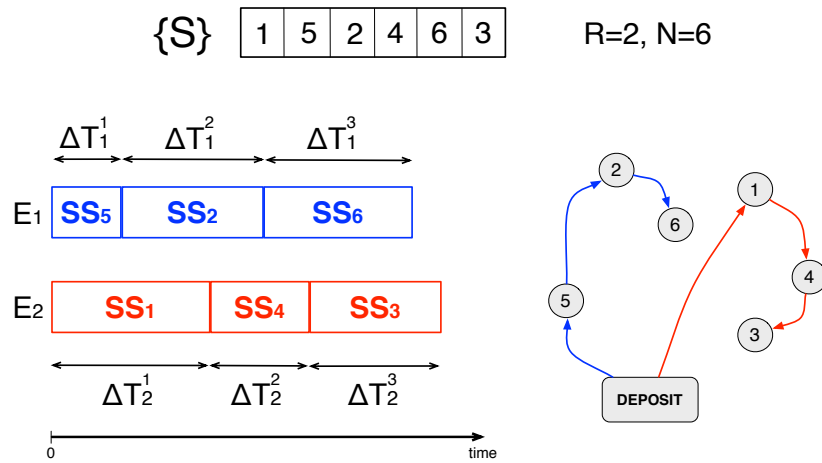


Figure 33: Case study: a candidate sequence solution for the optimization problem and a representation of the sequences of manual interventions over time.

Figure 33 shows a possible candidate sequence solution $\{S_m\}$ where we assume $N = 6$ manual interventions and $R = 2$ emergency teams.

It can be noticed that the generic time duration ΔT_m^j required to implement the manual intervention on the SS depends on the distance between the current SS (or deposit in case of the first intervention) and the arrival SS and on the traffic conditions in the area that covers the initial and the final SS.

Each restoration sequence thus produces a specific pattern of the set of $Q_k(t)$ which, in turn, influences the expected consequences through Eq. (24). Thus, the algorithm is able to measure the "quality" of the intervention providing a measure of the consequences which is able to produce. The operator will thus be able to choose the best sequence of restoration actions on the bases of their ultimate effects.

In order to assign an emergency team to the specific SS that requires manual intervention at time t_i , the reconfiguration algorithm (see Section 6.3) selects any emergency team that is available at time t_i . This is an important property as the impact Q_k and subsequently

the consequence C depend on the time durations required to reconnect the electrical users supplied by a certain SS . In other words, the more an emergency team takes to perform a manual intervention, the longer would be outage time and thus the worst would be the consequences for the citizens.

7.3 ORDINAL OPTIMIZATION BASED APPROACH

In this Section, we describe a resource allocation strategy to address the problem of resources allocation during a disaster event. In this case, the objective of the optimization is maximizing the operational capacity of a hospital.

Due to the huge combinatorial feasible search space, an Ordinal Optimization based approach is used to solve the problem using two main concepts: goal softening and order comparison. This approach aims at finding a Good Enough solution set (G) with an acceptable probability and efficient computational effort.

7.3.1 *Problem Overview*

The presented approach uses the DR-NEP-WebSimP simulation platform presented in chapter 3. In particular, infrastructure simulators are used to simulate the detailed topological configuration of the infrastructure. Specific calculations such as load flow analysis for power system and water steady state flow and pressure for water system are performed using the domain simulators. Disaster events are modeled in the simulators to find the available resources under these conditions.

The results of these calculations are then passed to the infrastructure simulator *i2Sim* to find the optimum allocation for the available resources.

7.3.1.1 *i2Sim Model*

The *i2Sim* model shows a high level abstraction of the disaster site where physical entities such as hospitals and power stations are modeled as cells connected by channels.

Each cell models its infrastructure using a non-linear input-output function described by *i2Sim* Human Readable Tables (HRT). The HRT determines the output of the cell, e.g., treated patients in a hospital, based on its physical damage and available input resources. The physical damage of the infrastructure caused by a disaster is modeled using *i2Sim* Physical Mode (PM) rating. Resources such as electricity and water are produced and consumed by the cells and transported by the channels. Flow of these resources can be controlled using *i2Sim* distributors outputs. The distribution ratios for the resources are de-

terminated by the optimization agent to represent the optimal allocation.

7.3.1.2 *Power System Model*

The power system model shows the details modeling parameters of a power distribution network for the disaster site. The model includes substations transformers, sectionalizing switches, alternate feeders, and loads. A radial topology is assumed since it is commonly used in the utilities. Loads are modeled as constant active power loads (constant P). The model uses load flow calculations to check feeders current and voltage limits. Failures in the power distribution network due to disaster can be modeled by faulty feeders or out-of-service transformers. The power system model is then used to calculate the available power to the critical infrastructure e.g., a hospital.

7.3.1.3 *Water System Model*

The water distribution model defines the modeling properties of the network that distributes water to different critical infrastructures (including a hospital) with appropriate quantity and pressure.

The model consists of different components including water storage facilities such as reservoirs and water tanks, a piping network for distribution of water to the consumers, valves to limit the pressure or flow at a specific point in the network, pumps to increase the water flow and output nodes where the water is consumed. Loads are modeled as constant water demand nodes. A failed pump or a broken pipe can be modeled to simulate failures in the water system due to a disaster. Newton-based global gradient algorithm (also known as the Todini and Pilati method [87]) is used to determine the water steady state in terms of water flows values at each pipe and hydraulic heads at each junction according to the water demand curve at each junction and considering the relative physical limits (e.g., pipes length, diameter). In order to simulate the behaviour of the water distribution network, the Epanet simulator [76] was used.

7.3.1.4 *Optimization Algorithm*

The optimization problem is based on Ordinal Optimization (OO), an optimization theory introduced by Ho et al. [47] to provide fast solutions for complex simulation based optimization problems.

Ordinal Optimization is based on two main concepts:

- Order Comparison: it is easier to determine order than value, i.e. determining $A > B$ is easier than determining the value of $A - B = ?$.
- Goal Softening: instead of looking for the best for sure, we look for good enough with high probability.

Using these two concepts, ordinal optimization methods provide a set of Good Enough solutions in an order of their performance. In many practical applications, it is enough to find good enough solutions instead of insisting on finding the true optimum solution which may exhaust the available computational resources. This rational motivates the application of ordinal optimization to the resources allocation problem addressed in this Section. After a crisis, disaster responders are under pressure to save lives and mitigate disaster impacts. In these emergency situations, they may accept a fast good enough solution instead of waiting for the optimum one.

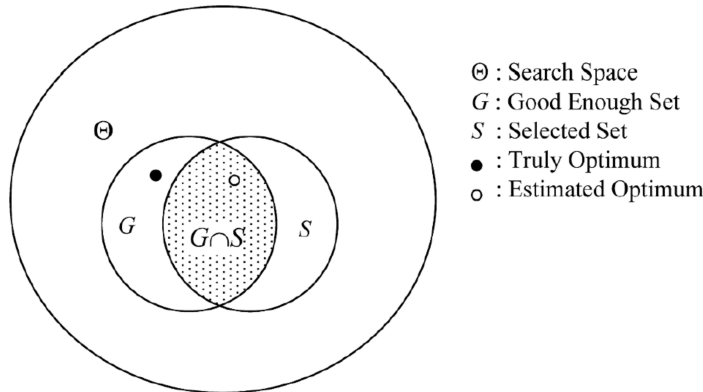


Figure 34: Ordinal Optimization solution space [47].

The key idea of ordinal optimization is to find a selected set $\{S\}$ of solutions with an acceptable probability to be a member of the good enough set G as shown in Figure 34. The good enough set is defined as the top n solution of the entire solutions space. Therefore, the problem is changed from finding the optimum resources distribution over the entire space to finding a set of distributions that has an overlap with the top n solutions in the entire solutions space Ω .

The resources allocation problem in disaster response is a combinatorial constraints optimization problem. The objective of the optimization problem is to maximize the number of saved lives. This function is represented by the output of the hospital model in i2Sim which measures the number of treated patients in the hospital.

In the first stage, we check for the solution feasibility. A solution is represented by a set of distribution ratios in i2Sim model. A feasible solution is a solution that does not violate resources supply constraints in the i2Sim model. We use the i2Sim model as a crude model to filter out unfeasible solutions and rank the feasible ones. Then, the Ordered Performance Curve (OPC) class and the good enough set G and the required alignment level K are determined.

In the second stage, we employ the domain simulators to check the physical constraints on the selected solutions. Typical physical con-

straints include voltage and current constraints in the power system and pressure constraint in the water system.

The optimization algorithm was implemented in MATLAB and integrated with the simulation models.

7.3.2 Case Study

The proposed approach was applied to a hypothetical disaster event. The i2Sim model consists of three production cells representing: a hospital that is fed by a power substation and a water pumping station. The power distribution supplies also the water pumping station.

A power distribution model was developed to map the power substation topology. The power model represents a typical radial configuration of distribution system with two supplying transformers and four feeders.

The water distribution network feeding the hospital represents an open radial topology with two independent water sources equipped with two pumps and one tank.

The disaster events were modeled by varying Physical Modes (PM) values in the i2Sim model. In i2Sim ontology, PM=1 means no damage to the infrastructure and PM=5 means completely damaged.

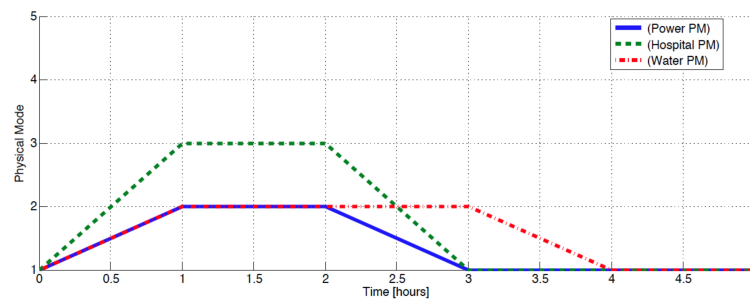


Figure 35: Curves trend of the Physical Modes of the i2sim model.

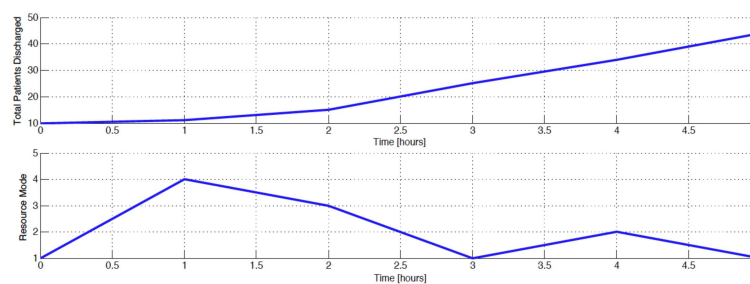


Figure 36: Hospital simulation results.

7.3.2.1 *Simulation Results*

Simulation scenario was assumed to have 5 hours duration with one hour time step. Results have shown that 44 patients can be treated in the hospital utilizing the available power and water resources in this scenario.

The hospitals output and values of its Resource Mode (RM) during the simulation are shown in Figure 35. RM value in i2Sim measures level of resources availability: RM=1 means all resources are available while RM=5 means no resources are available.

The algorithm calculates the best distribution ratios for the power and water distributors so that the operability of hospital is maximum. It can be seen from Figure 36 that hospitals output was affected by physical damages in the power substation and water station.

7.4 SIMULATION BASED APPROACH

7.4.1 *Problem Overview*

In this Section, we present a resource allocation strategy based on the DR-NEP-WebSimP simulation platform presented in chapter 3.

We demonstrate the utility of the platform using a case study involving power distribution to a hospital during a disaster event. The simulation platform presents decision makers with a set of feasible options. The three simulators, i2sim, PSS Sincal and ns-2, are used to model disaster events.

i2sim models a disaster event at a high level and assesses the effects of resource allocation. In a disaster scenario, i2sim maximizes the functionality of critical infrastructures (e.g., hospitals) by optimizing resource allocation. Different resources can be incorporated in i2sim models, such as electricity, water, medicine and transportation. In this case, we focus on the determination of the distribution of electricity using power grid and SCADA network infrastructure simulators.

The power grid is modeled using PSS Sincal, which simulates the status of the power system during a disaster event and examines the feasibility of possible configurations. The possible configurations include the power required to supply a load, electrical equipment used, power grid limits, and control elements of the SCADA communications network.

Resource allocation begins with i2sim suggesting the desired resource distribution required to supply a specific amount of electricity to a critical load (e.g., a hospital). Decisions are determined based on the i2sim optimization process, which considers other resources and critical infrastructures. PSS Sincal and ns-2 simulate the possible configurations that can accommodate an i2sim request and return a feasible configuration via the WebSimP adapter.

Note that the feasible configuration may or may not satisfy the initial request made by *izsim*. If all the conditions are not satisfied, *izsim* updates its model and selects another request. *PSS Sincal* and *ns-2* then simulate the configurations once again and return a feasible solution. The process continues iteratively to optimize the power distribution to critical infrastructures based on the power grid and SCADA network constraints.

7.4.2 Case Study

The case study involves a disaster event where the power and SCADA infrastructures place constraints on the resource allocation process. The main objective in the scenario is to maximize the operability of a hospital by providing the required electricity and water resources. The *izsim* simulates the interdependencies between the hospital and the water pumping station. *PSS Sincal* and *ns-2* simulate the physical constraints introduced by the power and SCADA networks.

In more complex situations, the failure of a power provider would affect multiple critical infrastructures. However, for demonstration purposes, we consider a small set of infrastructure entities.

7.4.2.1 Infrastructure Simulation Models

Power Distribution Grid. The power distribution grid shown in Figure 37 incorporates 165 buses, 22 circuit breakers and 46 loads. E_i represents the power transmission grid substations, P_i nodes represent high voltage (HV) 150 kV buses, M_i represent the medium voltage (MV) 20 kV buses, and physical links between two buses represent electrical lines. Each substation supplies energy to different types of loads/customers: (i) public loads/customers for the hospital, including emergency and intensive care units at very high criticality (M_{11} and M_{12}) and other hospital units (M_1, \dots, M_7); (ii) industrial loads/customers for a water pumping station and an industrial load (P_{20} and P_{24}); and residential loads/customers for domestic users (P_{12}).

In normal conditions, hospital loads are supplied by P_{13} and P_{26} through intermediate nodes M_i . In the event of a physical failure of P_{13} , the hospital is fed only through P_{26} . Since P_{26} can supply a maximum of 9.50 MW, load shedding actions must be initiated by the SCADA system to supply the hospital loads (Table 20).

SCADA system Figure 38 shows the SCADA system that controls the power distribution grid. The SCADA system includes: (i) a main SCADA control (MSC) center that controls and supervises the power distribution grid; (ii) a disaster recovery SCADA (DRS) center that assumes control and supervision in case of MSC failure; (iii) 44 re-

Table 20: Electricity demand for loads/customers.

Physical Entity	Electricity Demand (MW)
Hospital	13.47
Water Pumping Station	52.50
Industrial	9.47
Residential	120.91

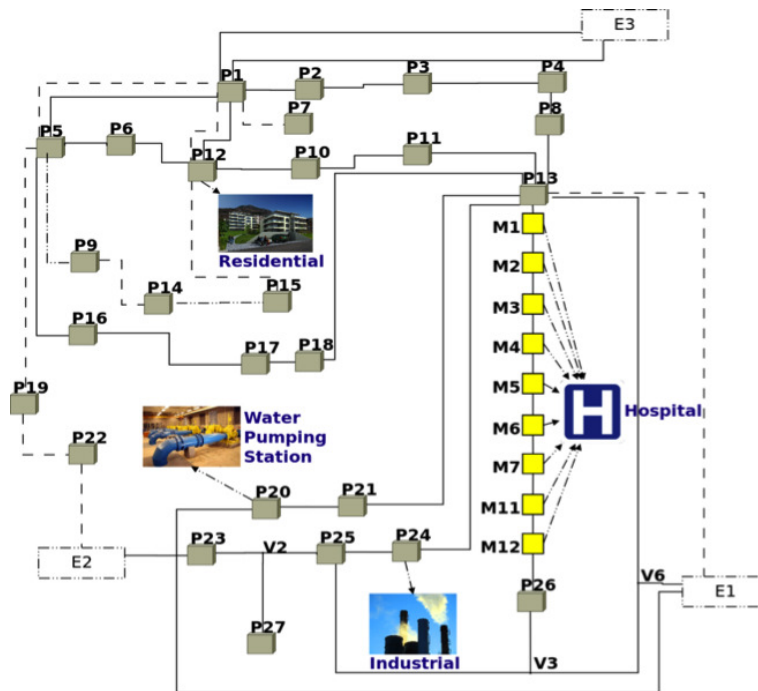


Figure 37: Power distribution grid and SCADA system.

note terminal units (RTUs) (P_i nodes) located at HV substations; and (iv) nine RTUs (M_i nodes) located at MV substations. RTUs receive commands through the SCADA communications network from the MSC and DRS centers to perform local actions on the power grid (e.g., closing circuit breakers). The SCADA communications network comprises two networks:

- The default proprietary network (DPN) connects the SCADA control centers to RTUs at the HV and MV substations. DPN nodes can also communicate with each other through the public switched telephone network (PSTN) to provide backup capabilities.
- The PSTN network models the public backup telecommunications network that connects the MSC and DRS to the HV RTUs. Two virtual private networks (VPNs) are established between the MSC and DRS via two high data rate digital subscriber line

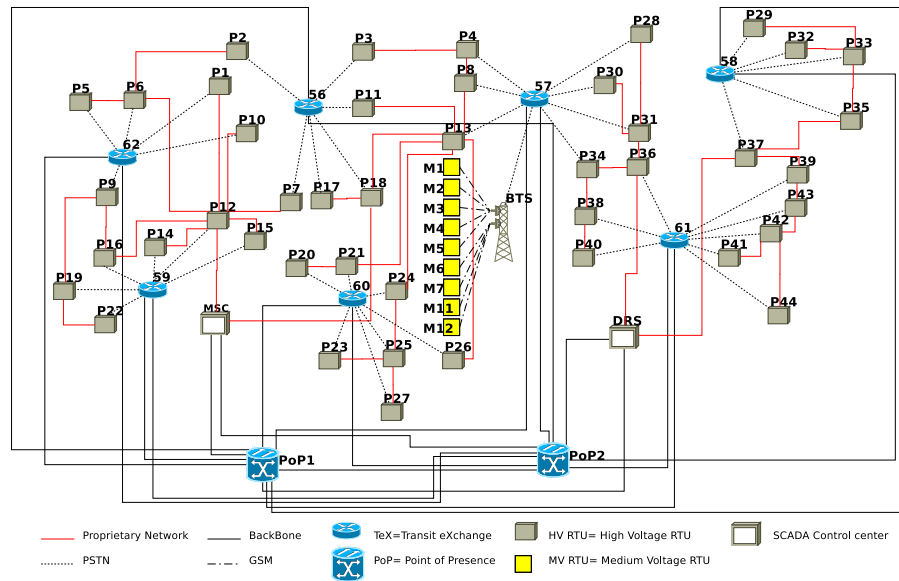


Figure 38: SCADA System.

Table 21: SCADA network model assumptions.

Link Type	Proprietary Network	PSTN	Backbone
Capacity	0,5 Mmps	0,5 Mmps	1 Mmps
Source-Destination	MSC – P_i , DRS – P_i ,	TeX _{<i>i</i>} – P_j	PoP _{<i>i</i>} – PoP _{<i>j</i>} , PoP _{<i>i</i>} – TeX _{<i>j</i>} ,
Nodes	P_i – P_j , P_i – M_j , M_i – M_j ,		MSC – PoP _{<i>i</i>} , DRS – PoP _{<i>i</i>} ,
Traffic Type	CBR over TCP	CBR over TCP	CBR over TCP
Traffic Bit Rate	255 B / 30 sec	255 B / 30 sec	255 B / 30 sec

connections that employ two points of presence (PoPs), PoP₁ and PoP₂. . . .

Communications between the MSC and DRS and the RTUs are modeled with ns-2 using TCP agents located at the source and destination nodes. Traffic is generated at a specified constant bit rate (CBR). Table 21 summarizes the main assumptions.

izsim Model The I2Sim model provides a high-level abstraction of the physical components. The detailed topological configurations of the power and SCADA networks are modeled using the domain simulators, PSS Sincal and ns-2, respectively. In the I2Sim ontology, physical infrastructure entities are modeled as cells connected by channels that transport resources (e.g., electricity and water). In the model shown in Figure 39, eight cells are used to represent interdependent

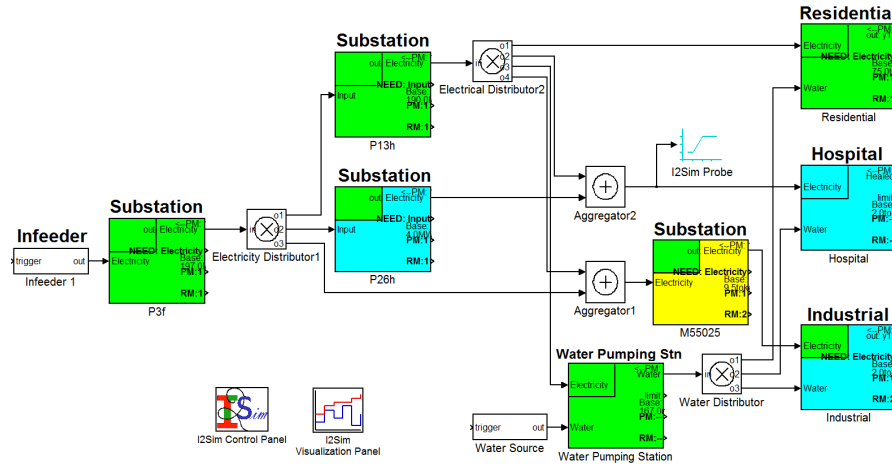


Figure 39: i2sim Model.

Table 22: Sequence of events for the simulated scenarios.

No.	Time	Event	Effect
1	T1	Normal operation	Hospital and water pumping station have full supply of electricity and water
2	T2	Equipment failure is detected	Hospital loads lose 6.2MW of supply
3	T3	Feasible configuration of power grid is implemented	Hospital and water pumping station loads are partially supplied
4	T4	Affected equipment is restored	Full supply can be restored
5	T5	Normal operation configuration is restored	Hospital and water pumping station have full supply of electricity and water

infrastructures at the disaster site, consisting of four electrical substations, a water pumping station, a hospital, residential loads and industrial loads.

7.4.2.2 Simulation Scenarios

Three scenarios are simulated to illustrate the utility of the DR-NEP platform. All three scenarios involve a transformer failure in the power grid. However, two of the scenarios, Scenario 2 and Scenario 3, are more severe in that they also involve failures of SCADA network components.:

- Scenario 1: A failure in the power grid (transformer) only.

Table 23: Feasible configurations for 100% power supply to the water pumping station.

No.	Power Supply	Feasible Configurations
1	100%	Configuration 1: Breakers P_{10} , P_{13} and P_{26} closed, and all tie breakers in $M_1 - M_{12}$ are closed
2	75%	Configuration 2: Breaker P_{13h} open, breaker P_{26h} closed, breakers ($M_1 - M_2 - M_5 - M_6 - M_{11} - M_{12}$) closed, breakers ($M_3 - M_4 - M_7$) open Configuration 3: Breaker P_{13} open, breaker P_{26} closed, breakers ($M_1 - M_2 - M_3 - M_5 - M_{11} - M_{12}$) closed, breakers ($M_4 - M_6 - M_7$) open Configuration 4: Breaker P_{13} open, breaker P_{26} closed, breakers ($M_5 - M_6 - M_7 - M_{11} - M_{12}$) closed, breakers ($M_1 - M_2 - M_3 - M_4$) open
3	50%	Configuration 5: Breaker P_{13} open, breaker P_{26} closed, breakers ($M_1 - M_2 - M_{11} - M_{12}$) closed, breakers ($M_3 - M_4 - M_5 - M_6 - M_7$) open
4	25%	Configuration 6: Breaker P_{13} open, breaker P_{26} closed, breakers ($M_{11} - M_{12}$) closed, breakers ($M_1 - M_2 - M_3 - M_4 - M_5 - M_6 - M_7$) open
5	0%	Configuration 7: Breakers P_{13} and P_{26} open

- Scenario 2: A failure in the power grid (transformer) with a failure in the SCADA network (RTU);
- Scenario 3: A failure in the power grid (transformer) with two failures in the SCADA network (RTU and communications node);

Table 22 shows the sequence of events for the three scenarios. At time T_2 , failures are introduced: a transformer in Scenario 1; a transformer and an RTU in Scenario 2; and a transformer, RTU and communications node in Scenario 3. At time T_3 , a desired configuration of the power grid, selected by I2Sim, is sent to the domain simulators for verification. Note that the desired configuration is selected based on optimality, experience and pre-determined feasibility of the power grid and SCADA networks.

The I2Sim ontology defines operability in terms of available resources in human readable tables with five levels: 100%, 75%, 50%, 25%, and 0%. Note that the hospital and water pumping station require 100% power supply for full operability. However, 100% power supply may not be possible during disasters due to damage to the physical systems. In such situations, different combinations of the distributions of available resources can be deployed (e.g., 75% power

Table 24: Decision space for the three scenarios.

Scenario 1					
	100%	75%	50%	25%	0%
100%	X	X	X	X	X
75%	X	X	X	X	X
50%	X	X	X	X	X
25%	X	X	X	X	X
0%	X	X	X	X	X

Scenario 2					
	100%	75%	50%	25%	0%
100%	X	X	X	X	X
75%	X	X	X	X	X
50%	X	X	X	X	X
25%	X	X	X	X	X
0%	X	X	X	X	X

Scenario 3					
	100%	75%	50%	25%	0%
100%	X	X	X	X	X
75%	X	X	X	X	X
50%	X	X	X	X	X
25%	X	X	X	X	X
0%	X	X	X	X	X

supply to the hospital and 50% power supply to the water pumping station).

In the three scenarios, the distribution of electricity between the hospital and the water pumping station is determined based on the physical constraints of the power grid and SCADA networks. For example, Table 23 shows the feasible configurations for 100% power supply to the water pumping station and different power supply percentages to the hospital.

7.4.2.3 Simulation Results

Based on the five levels in the human readable tables, there are $5 \times 5 = 25$ possible combinations for electricity distribution between the hospital and the water pumping station. However, the failures in the power grid and SCADA networks limit the set of feasible configurations. Table 24 compares the decision spaces for the three simulated scenarios in terms of the number of feasible configurations available for each scenario. The rows represent the levels of power supplied to the hospital and the columns represent the levels of power sup-

Table 25: Simulation results.

No.	Configuration	EF	SF	GF	Rt (sec)
Scenario 1	1 (100%)	NO	YES	NO	-
	2 (75%)	YES	YES	YES	420.4
Scenario 2	1 (100%)	NO	NO	NO	-
	2 (75%)	YES	NO	NO	-
	3 (50%)	YES	NO	NO	-
	4 (50%)	YES	YES	YES	367.4
Scenario 3	1 (100%)	NO	NO	NO	-
	2 (75%)	YES	NO	NO	-
	3 (50%)	YES	NO	NO	-
	4 (50%)	YES	NO	NO	-
	5 (50%)	YES	NO	NO	-
	6 (25%)	YES	NO	NO	-
	7 (0%)	YES	YES	YES	0

plied to the water pumping station. The boldface X symbols denote the feasible combinations for electricity distribution. In Scenario 1, for example, a maximum 75% power supply can be delivered to the hospital and the water pumping station.

Table 24 presents the results of the resource allocation process. Note that EF denotes electrical feasibility, SF denoted SCADA feasibility, GF denotes global feasibility and Rt denotes reconfiguration time. Configuration 1 in Scenario 1 is not electrically feasible because feeder P₁₃ is isolated from the network by the transformer failure and the power required to supply all the M_i loads cannot be provided through feeder P₂₆ because of the electrical constraints (P₂₆ cannot exceed its 9.50 MW capacity). On the other hand, Configuration 2 in Scenario 1 has global feasibility (marked with a boldface Yes). This means that all the components of the power grid are within their physical limits and a communication path between the MSC and RTUs is available.

The time required for reconfiguring the power grid was computed by considering the physical time needed to open/close breakers plus the SCADA message round trip time (RTT). The simulated scenarios show that the RTT is negligible with respect to breaker operation. The open/close operations take 50 seconds for MV breakers and 100 seconds for HV breakers.

7.5 CHAPTER SUMMARY

In this Chapter, we address the final stage in the disaster response process: to make the best possible decisions once the state of damage

of the system is known and the available resources are known. The problem at this point becomes an optimization problem on how to allocate the available resources to improve response effectiveness.

System optimization theory is well developed. However, in a disaster situation, optimization has to be achieved not over well-defined punctual states of the system, but over a number of hours (or days) in the timeline of the disaster, while additional events may occur and disturb the system along this timeline. In these scenarios, decision makers may be in favour of taking fast suboptimal decisions versus one global best decisions in order to take immediate countermeasures.

In Section 7.2, we have shown that during disaster scenarios, optimization of the available resources (e.g., electrical power, emergency teams) approaches that take into account the existing interdependency phenomena can decrease the negative consequences for the more vulnerable areas of population (e.g., old aged people, children, disabled people) that should be better protected against risks derived by the lack of primary services (e.g., hospitals).

In Section 7.3, a simulation-based tool for helping disaster responders was proposed. The simulation platform was used to take infrastructures interdependencies into consideration. An Ordinal Optimization based approach was developed to find the optimal allocation of resources, power and water, for a disaster event. The output of a hospital in terms of number of discharged patients was taken as a performance measure.

In Section 7.4, we presented a disaster response planning simulation platform described providing decision support based on the interdependencies existing between a power grid and a SCADA system. The platform offers a powerful interactive simulation environment for disaster response planning, enabling planners to evaluate specific scenarios and select the appropriate responses.

Part III

EPILOGUE

CONCLUSIONS

Wireless sensor networks are increasingly used to monitor critical infrastructure assets, including power networks and dams. They may expose SCADA systems to new threats introduced by the information and communications technology layer. Unlike traditional sensor systems, wireless sensor networks are also vulnerable to cyber attacks affecting confidentiality, integrity and availability of sensitive data.

Moreover, natural hazards including hydrological (e.g., drought, floods), geological (e.g., earthquakes, landslides and volcanoes), climatic and atmospheric (e.g., extremes of heat and cold, windstorm) hazards can seriously disrupt critical infrastructures.

To cope with these threats and reduce the possibility of cascading failures, it is important to implement resilience at each infrastructure level so that an effective response to emergencies can be enabled.

The work presented in this dissertation provides a comprehensive risk analysis workflow for disaster situations: from the initial detection implemented through sensors networks to an optimized response that takes into account the "wealth" of the citizens, the economy, the delivery of primary services (e.g., schools, hospitals, public transportations, activities of the public administration), and the environment.

The study of data fusion techniques inside the evidence theory framework, enriches the critical infrastructure models with the possibility of merging data regarding the occurrence of adverse events (e.g., physical security threats) and thus producing more informative information given by early warnings. Such information may be valuable for decision makers to take appropriate countermeasures immediately after the occurrence of the events.

In addition, these information can be used by interdependency models that offer a higher level of situation awareness as they predict the near future degradation levels of services provided by the infrastructures by keeping into account not only the raw information coming from the sensors (e.g., the quantity of a current rainfall in an electric substation or a cyber intrusion in a SCADA system) but also the interdependency phenomena.

Enabling these capabilities inside a Decision Support System equipped with geo-referential information of the monitored infrastructures, the territory, and the census data may also be used to evaluate the ultimate consequences for the society.

An additional level of response to emergencies can also be provided to decision makers through the development of strategies to opti-

mally allocate resources or to reach a disaster area following the minimum path.

This work will help the disaster response community to better understand all aspects involved in disaster management and will hopefully lead to policy decisions that will ameliorate the consequences of nature-driven disasters and man-driven malicious attacks.

Part IV

APPENDIX

PROOFS

A.1 LEMMA 1 PROOF

Proof. In order to prove the convergence of the proposed algorithm towards a steady-state, let us consider a generic network topology where $|V| = N$ representing the number of agents, that is critical infrastructures in our case.

Let us consider the network at different time intervals $[t_0, t_0 + \Delta t_0]$, $[t_1, t_1 + \Delta t_1]$, ..., $[t_h, t_h + \Delta t_h]$ with $t_1 = t_0 + \Delta t_0 + 1$, $t_h = t_{h-1} + \Delta t_{h-1} + 1$. During each time interval Δt_i , the agents interact using the interaction rule \mathcal{R} to form a connected graph.

In particular, for any pair v_i and v_j such that $(v_i, v_j) \in \mathcal{E}(t)$ at time t , the cautious rule of combination is applied so that the two agents agree on the minimum of the weight function set values i.e.:

$$s_i(t) \bigwedge s_j(t) = (w_{1 \otimes 2}(t, \gamma_1), \dots, w_{1 \otimes 2}(t, \gamma_z)) \quad (26)$$

with $z = |2^\Omega \setminus \Omega|$ as defined in (11).

With no lack of generality, let us consider γ_a and assume that \exists an agent v_q s.t. $w_q(0, \gamma_a) = \bar{w}(0, \gamma_a) \leq w_m(0, \gamma_a)$ with $v_m \in \mathcal{V}$. Considering that, at each iteration, all the $w(t, \gamma_a)$ with $\gamma_a \in 2^\Omega \setminus \Omega$ are compared among two agents to find the minimum, therefore let us to focus our reasoning on a generic γ_a .

Let us consider, for each time interval Δt_k , a particular edge selection policy that updates only *one* agent to $\bar{w}(t_k, \gamma_a)$. In addition, let us consider a partition of $P = \{U, W\}$ of \mathcal{V} with $U, W \subseteq \mathcal{V}$, $U \cap W = \emptyset$, $U \cup W = V$ where U contains the set agents that have reached the $\bar{w}(t_k, \gamma_a)$ and $W = V \setminus U$ the set of the remaining agents.

The worst case scenario for the edge selection policy ϵ , in terms of number of interactions required to update only the state of *one* agent, verifies when the connection between two agents $v_u \in U$ and $v_w \in W$, for which $e_{uv} = (v_u, v_w) \in \mathcal{E}'(t_k, t_k + \Delta t_k)$, occurs as *last* interaction and the graph $\mathcal{G}'(t_k + \Delta t_k) = \{U \cup W, \mathcal{E}'(t_k, t_k + \Delta t_k)\}$, with $e_{uv} \in \mathcal{E}'(t_k, t_k + \Delta t_k)$, is connected.

Let us now consider the worst case topology for a network with N agents, that is the topology for which the larger numbers of updates is required to reach convergence when the worst case edge selection policy is considered. Clearly, the worst case scenario is the topology with the largest diameter, i.e., the line topology.

In addition, let us consider the worst case scenario for the topology, in terms of number of interactions required to update one agent to $\bar{w}(t_i, \gamma_a)$ and obtain a connected graph within a time interval Δt_i .

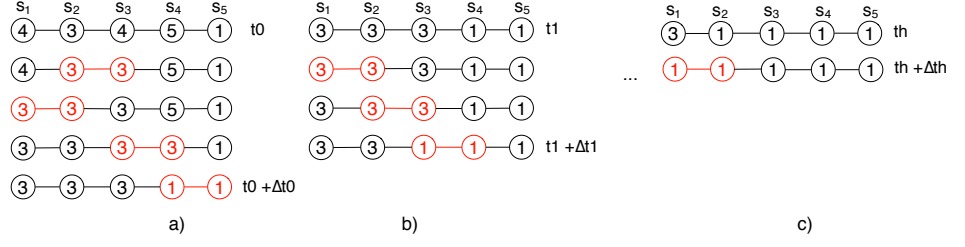


Figure 40: Steady-state convergence at different time-intervals. The number inside each circle represents the weight function set value $w_i(t_i, \gamma_a)$ of a generic set $\gamma_a \in 2^\Omega \setminus \Omega$, associated to agent i .

This particular topology is the one that exhibits the longest diameter d , that, allows only for one update at each time interval. Clearly, this topology is given by a line with $d = N - 1$, as shown in Figure 40 where the agent with $\bar{w}(t_i, \gamma_a)$ is placed on the extreme right so that the longest diameter is obtained.

Now, let us consider a time interval $[t_0, t_0 + \Delta t_0]$. With no lack of generality, let us consider, at time t_0 , $|W| = N - 1$ and $|\mathcal{U}| = 1$. At exact time $t_0 + \Delta t_0$, two agents $v_u \in \mathcal{U}$ and $v_w \in W$ communicate as last iteration so that $|W| = N - 2$ and $|\mathcal{U}| = 2$ rendering the graph $\mathcal{G}'(t_0 + \Delta t_0) = \{\mathcal{U} \cup W, \mathcal{E}'(t_0, t_0 + \Delta t_0)\}$ connected. Now, let us consider a new time interval $[t_1, t_1 + \Delta t_1]$. At time t_1 , $|W| = N - 2$ and $|\mathcal{U}| = 2$. By iterating the same reasoning for the edge selection policy, at exact time $t_1 + \Delta t_1$, two agents $v_u \in \mathcal{U}$ and $v_w \in W$ communicate as last iteration so that so that $|W| = N - 3$ and $|\mathcal{U}| = 3$ rendering the graph $\mathcal{G}'(t_1 + \Delta t_1) = \{\mathcal{U} \cup W, \mathcal{E}'(t_1, t_1 + \Delta t_1)\}$ connected.

Now, let us consider a new time interval $[t_h, t_h + \Delta t_h]$. At time t_h , $|W| = N - (h + 1)$ and $|\mathcal{U}| = h + 1$. By iterating the same reasoning for the edge selection policy, at exact time $t_{N-1} + \Delta t_{N-1}$, two agents $v_u \in \mathcal{U}$ and $v_w \in W$ communicate as last iteration so that $|W| = 0$ and $|\mathcal{U}| = N$ rendering the graph $\mathcal{G}'(t_{N-1} + \Delta t_{N-1}) = \{\mathcal{U} \cup W, \mathcal{E}'(t_{N-1}, t_{N-1} + \Delta t_{N-1})\}$ connected. At this point, all the agents v_i for $i = 1..N$ will have reached the same state $s(t') = \{\bar{w}(t', \gamma_a); \gamma_a \in 2^\Omega \setminus \Omega\}$. Therefore, $s(t')$ is a steady state for the multi-agent system.

In Figure 40, we show the steady-state convergence at different time steps for the worst network topology with $N = 5$. Considering that, within each time interval Δt_i , only one agent is updated, this implies that $d \cdot \Delta t_i$, where d is the diameter of the network, is the number of time intervals $[t_i, t_i + \Delta t_i]$ where all the nodes are updated. □

A.2 LEMMA 2 PROOF

Proof. The Proof follows directly from Lemma 1. In particular, we recall that, in the worst case scenario for the topology, the network

exhibits the largest diameter d so that $d = N - 1$ and $d \cdot \Delta t_i$ is the number of time intervals $[t_i, t_i + \Delta t_i]$ where all the nodes are updated. Assuming that an upper bound M is available to the time required for the network to be connected within each time interval $[t_i, t_i + \Delta t_i]$, the time required to update one agent is $t_i = M$. By iterating the same reasoning, the process takes $t = d \cdot M$ to update all agents. Therefore, the overall time required to the algorithm to converge in the worst case scenario for the topology is linear w.r.t. the diameter of the network topology \mathcal{G} .

□

BIBLIOGRAPHY

- [1] OPSAID Initial Design and Testing Report. Technical report, US Department of Energy Office of Electric Delivery and Reliability Os National SCADA Testbed Program, 2009.
- [2] EU FP7 MICIE project, 2010. URL <http://www.micie.eu>.
- [3] EU FP7 CockpitCI project, 2012. URL <http://www.cockpitci.eu>.
- [4] The network simulator ns-2, 2012. URL <http://www.isi.edu/nsnam/ns/ns-documentation.html>.
- [5] SimTec, PSS SINICAL Platform, 2012. URL http://www.simtec-gmbh.at/sites_en/sinical_updates.asp.
- [6] EU FP7 UrbanFlood Project, 2012. URL <http://www.urbanflood.eu>.
- [7] European Flood Awareness System (EFAS)., 2015. URL <https://www.efas.eu/>.
- [8] General Electric, iFIX HMI/SCADA, 2015. URL <http://support.geip.com/support/index?page=prohome&cat=HMISCADAIFIX>.
- [9] INGV, Italian National Institute of Geophysics and Volcanology., 2015. URL <http://www.ingv.it/>.
- [10] Rose A., Oladosu G., and Liao S. In *2th annual symposium of the DHS center for risk and economic analysis of terrorism events*, 2005.
- [11] A. Alsubaie, A. Di Pietro, J. Marti, P. Kini, Ting Fu Lin, S. Palmieri, and A. Tofani. A platform for disaster response planning with interdependency simulation functionality. In *Critical Infrastructure Protection VII - 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers*, pages 183–197, 2013. doi: 10.1007/978-3-642-45330-4_13. URL http://dx.doi.org/10.1007/978-3-642-45330-4_13.
- [12] H. Arora, T.S. Raghu, and A. Vinze. Resource allocation for demand surge mitigation during disaster response. *Decision Support Systems*, 50(1):304 – 315, 2010. ISSN 0167-9236. doi: <http://dx.doi.org/10.1016/j.dss.2010.08.032>. URL <http://www.sciencedirect.com/science/article/pii/S0167923610001569>.
- [13] N. Basu, R. Pryor, and T. Quint. Aspen: A microsimulation model of the economy. *Comput. Econ.*, 12(3):223–241, December 1998. ISSN 0927-7099. doi: 10.1023/A:1008691115079. URL <http://dx.doi.org/10.1023/A:1008691115079>.

- [14] S. P. Boyd, A. Ghosh, B. Prabhakar, and D. Shah. Randomized gossip algorithms. *IEEE Transactions on Information Theory*, 52(6): 2508–2530, 2006.
- [15] F. Caldeira, M. Castrucci, M. Aubigny, D. Macone, E. Monteiro, F. Rente, P. Simoes, and V. Suraci. Secure mediation gateway architecture enabling the communication among critical infrastructures. In *Future Network and Mobile Summit, 2010*, pages 1–8, June 2010.
- [16] J.O. Calvin and R Weatherly. An introduction to the High Level Architecture (HLA) runtime infrastructure (RTI). In *Proceedings of the 14th Workshop on Standards for the Interoperability of Defence Simulations*, pages 705–715, Orlando, FL, USA, 1996.
- [17] F. Castanedo. A review of data fusion techniques. *The Scientific World Journal*, 2013, October 2013. doi: 10.1155/2013/704504. URL <http://www.hindawi.com/journals/tswj/2013/704504/abs/>.
- [18] R. Chabukswar, B. Sinopoli, G. Karsai, A. Giani, H. Neema, and A. Davis. Simulation of Network Attacks on SCADA Systems. In *First Workshop on Secure Control Systems, Cyber Physical Systems Week 2010*, 04/2010 2010. URL <http://www.truststc.org/pubs/693.html>.
- [19] V. Cherfaoui, T. Denoeux, and Z.L. Cherfi. Distributed data fusion: application to confidence management in vehicular networks. In *Information Fusion, 2008 11th International Conference on*, pages 1–8, June 2008.
- [20] V. Cherfaoui, T. Denoeux, and Z.-L. Cherfi. *Confidence Management in Vehicular Network*, x Confidence Management in Vehicular Network, pages 357–378. CRC Press. Taylor and Francis, 2009. ISBN: 9781420085716.
- [21] Wang Chunlei, Fang Lan, and Dai Yiqi. A simulation environment for SCADA security analysis and assessment. In *Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on*, volume 1, pages 342–347, March 2010. doi: 10.1109/ICMTMA.2010.603.
- [22] N. Collier. Repast: An extensible framework for agent simulation. *Natural Resources and Environmental Issues*, (4), 2001.
- [23] Subrata Das. *High-Level Data Fusion*. Artech House Publishers, Sep 2008. ISBN 1596932813. URL <http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/1596932813>.
- [24] C.M. Davis, J.E. Tate, H. Okhravi, C. Grier, T.J. Overbye, and D. Nicol. SCADA Cyber Security Testbed Development. In *Power*

- Symposium, 2006. NAPS 2006. 38th North American*, pages 483–488, Sept 2006. doi: 10.1109/NAPS.2006.359615.
- [25] S. De Porcellinis, G. Oliva, S. Panzieri, and R. Setola. A holistic-reductionistic approach for modeling interdependencies. In Charles Palmer and Sujeet Sheno, editors, *Critical Infrastructure Protection III*, volume 311 of *IFIP Advances in Information and Communication Technology*, pages 215–227. Springer Berlin Heidelberg, 2009. ISBN 978-3-642-04797-8. doi: 10.1007/978-3-642-04798-5_15. URL http://dx.doi.org/10.1007/978-3-642-04798-5_15.
- [26] L. D. Decanini and F. Mollaioli. Formulation of elastic earthquake input energy spectra. *Earthquake Engineering and Structural Dynamics*, 27(12):1503–1522, 1998. ISSN 1096-9845.
- [27] A. P. Dempster. A generalization of bayesian inference. *Journal of the Royal Statistical Society*, 30(B):205–247, 1968.
- [28] A. P. Dempster. Upper and lower probabilities induced by a multivalued mapping. In *Classic Works of the Dempster-Shafer Theory of Belief Functions*, pages 57–72. 2008.
- [29] T. Denoeux. Conjunctive and disjunctive combination of belief functions induced by nondistinct bodies of evidence. *Artificial Intelligence*, 172(2-3):234 – 264, 2008. ISSN 0004-3702.
- [30] B. Ducourthial, V. Cherfaoui, and T. Denoeux. Self-stabilizing distributed data fusion. In Andrea W. Richa and Christian Scheideler, editors, *Stabilization, Safety, and Security of Distributed Systems*, volume 7596 of *Lecture Notes in Computer Science*, pages 148–162. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-33535-8.
- [31] L. Duenas-Osorio, J. I. Craig, and B. J. Goodno. Seismic response of critical interdependent networks. *Earthquake Engineering & Structural Dynamics*, 36(2):285–306, 2007. ISSN 1096-9845. doi: 10.1002/eqe.626. URL <http://dx.doi.org/10.1002/eqe.626>.
- [32] G. Dunning. *Programming the Controllogix Programmable Automation Controller Using RSLogix 5000 Software*. Cengage Learning, 2008. ISBN 9781401884321. URL <http://books.google.it/books?id=MUfaweUUzyQC>.
- [33] E.C. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Ojeu, European Commission, 2008.
- [34] M. R. Endsley. Design and evaluation for situation awareness enhancement. In *Proc. of the Human Factors Society 32nd Annual Meeting*, pages 97–101, Santa Monica, CA, U.S.A., 1988.

- [35] I. Eusgeld and Nan Cen. Adopting HLA standard for interdependency study. *Reliability Engineering & System Safety*, 96(1):149 – 159, 2011. ISSN 0951-8320. doi: <http://dx.doi.org/10.1016/j.ress.2010.08.002>. URL <http://www.sciencedirect.com/science/article/pii/S0951832010001870>. Special Issue on Safe-comp 2008.
- [36] I. Eusgeld, Nan Cen, and Dietz S. System-of-systems approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6):679 – 686, 2011. ISSN 0951-8320. doi: <http://dx.doi.org/10.1016/j.ress.2010.12.010>. URL <http://www.sciencedirect.com/science/article/pii/S0951832010002668>. {ESREL} 2009 Special Issue.
- [37] N. Falliere and Liam O. W32.Stuxnet Dossier, 2011. URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
- [38] F. Fiedrich. An HLA-Based multiagent system for optimized resource allocation after strong earthquakes. In *Simulation Conference, 2006. WSC 06. Proceedings of the Winter*, pages 486–492, Dec 2006. doi: 10.1109/WSC.2006.323120.
- [39] F. Fiedrich, F. Gehbauer, and U. Rickers. Optimized resource allocation for emergency response after earthquake disasters. *Safety Science*, 35(1–3):41 – 57, 2000. ISSN 0925-7535. doi: [http://dx.doi.org/10.1016/S0925-7535\(00\)00021-7](http://dx.doi.org/10.1016/S0925-7535(00)00021-7). URL <http://www.sciencedirect.com/science/article/pii/S0925753500000217>.
- [40] F. Flammini, A. Gaglione, N. Mazzocca, V. Moscato, and C. Pragliola. Wireless sensor data fusion for critical infrastructure security. In Emilio Corchado, Rodolfo Zunino, Paolo Gastaldo, and Alvaro Herrero, editors, *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISISo8*, volume 53 of *Advances in Soft Computing*, pages 92–99. Springer Berlin Heidelberg, 2009. ISBN 978-3-540-88180-3. doi: 10.1007/978-3-540-88181-0_12. URL http://dx.doi.org/10.1007/978-3-540-88181-0_12.
- [41] C. Foglietta, A. Gasparri, and S. Panzieri. A networked evidence theory framework for critical infrastructure modeling. In Jonathan Butts and Sujeet Sheno, editors, *Critical Infrastructure Protection VI*, volume 390 of *IFIP Advances in Information and Communication Technology*, pages 205–215. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-35763-3.
- [42] A. Gasparri, F. Fiorini, M. Di Rocco, and S. Panzieri. A networked transferable belief model approach for distributed data aggregation. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 42(2):391–405, April 2012. ISSN 1083-4419.

- [43] B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera. Analyzing cyber-physical attacks on networked industrial control systems. In Jonathan Butts and Sujeet Sheno, editors, *Critical Infrastructure Protection*, volume 367 of *IFIP Advances in Information and Communication Technology*, pages 167–183. Springer, 2011. ISBN 978-3-642-24863-4. URL <http://dblp.uni-trier.de/db/conf/ifip11-10/iccip2011.html#GengeFSM11>.
- [44] S. Giovinazzi and S. Lagomarsino. Sensor networks for monitoring and control of water distribution systems. *Proc. 10th Italian conference on earthquake engineering*, 2001. (in Italian).
- [45] Y. Haimes and P. Jiang. Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure Systems*, 7(1):1–12, 2001. doi: 10.1061/(ASCE)1076-0342(2001)7:1(1). URL [http://dx.doi.org/10.1061/\(ASCE\)1076-0342\(2001\)7:1\(1\)](http://dx.doi.org/10.1061/(ASCE)1076-0342(2001)7:1(1)).
- [46] J. Hasler. Investigating russia’s biggest dam explosion: What went wrong. *Popular Mechanics*, Feb 2010.
- [47] Y.C. Ho, Q.C. Zhao, and Q.S. Jia. *Ordinal Optimization: Soft Optimization for Hard Problems*. The International Series on Discrete Event Dynamic Systems. Springer, 2007. ISBN 9780387372327. URL http://books.google.ca/books?id=X_0XoVMgM_8C.
- [48] J. H. Holland. *Adaptation in Natural and Artificial Systems*. MIT Press, Cambridge, MA, USA, 1992. ISBN 0-262-58111-6.
- [49] G. Lanzano, E. Salzano, F. Santucci De Magistris, and G. Fabbrocino. Vulnerability of pipelines subjected to permanent deformation due to geotechnical co-seismic effects. *Chemical Engineering Transactions on*, 32, 2013.
- [50] J.C. Laprie, K. Kanoun, and M. Kaaniche. Modelling interdependencies between the electricity and information infrastructures. In F. Saglietti and N. Oster, editors, *Computer Safety, Reliability, and Security*, volume 4680 of *Lecture Notes in Computer Science*, pages 54–67. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-75100-7. doi: 10.1007/978-3-540-75101-4_5. URL http://dx.doi.org/10.1007/978-3-540-75101-4_5.
- [51] E.E. Lee, J.E. Mitchell, and W.A. Wallace. Restoration of services in interdependent infrastructure systems: A network flows approach. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 37(6):1303–1317, Nov 2007. ISSN 1094-6977. doi: 10.1109/TSMCC.2007.905859.
- [52] W. W. Leontief. Input-Output Economics. *Scientific American*, 185:15–21, October 1951. doi: 10.1038/scientificamerican1051-15.

- [53] L. Liu. Prototyping and cells modelling of the infrastructures interdependencies simulator izsim. Master's thesis, University of British Columbia, British Columbia, Canada, Aug 2007.
- [54] W.P. Luan, M.R. Irving, and J.S. Daniel. Genetic algorithm for supply restoration and optimal load shedding in power system distribution networks. *Generation, Transmission and Distribution, IEE Proceedings-*, 149(2):145–151, Mar 2002. ISSN 1350-2360. doi: 10.1049/ip-gtd:20020095.
- [55] J. R. Marti, P. Kini, P. Lusina, A. Di Pietro, B. Charnier V. Rosato and, and K. Wang. Inter-system software adapter for decision support by interfacing disaster response platforms and simulation platforms. In *Global Humanitarian Technology Conference (GHTC), 2012 IEEE*, pages 41–46, Oct 2012. doi: 10.1109/GHTC.2012.16.
- [56] E. Martin, D. Liggins, L. Hall, and J. Llinas. *Handbook of multisensor data fusion: theory and practice*, volume 22. CRC Press, 2008.
- [57] T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, and D. Reed. Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems*, 13(3):175–184, 2007. doi: 10.1061/(ASCE)1076-0342(2007)13:3(175). URL [http://dx.doi.org/10.1061/\(ASCE\)1076-0342\(2007\)13:3\(175\)](http://dx.doi.org/10.1061/(ASCE)1076-0342(2007)13:3(175)).
- [58] M.J. McDonald, G.N. Conrad, T.C. Service, and R.H Cassidy. Cyber effects analysis using vcse D promoting control system reliability. Technical report, Sandia National Laboratories Report (SAND2008-5954), 2008.
- [59] I. Nai Fovino, M. Masera, L. Guidi, and G. Carpi. An experimental platform for assessing scada vulnerabilities and countermeasures in power plants. In *Human System Interactions (HSI), 2010 3rd Conference on*, pages 679–686, May 2010. doi: 10.1109/HSI.2010.5514494.
- [60] A. Nieuwenhuijs, E. Luijff, and K. Marieke. Modeling dependencies in critical infrastructures. In *Critical Infrastructure Protection II - Second Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, George Mason University, Arlington, Virginia, USA, March 17-19, 2008, Revised Papers*, pages 205–213, 2008.
- [61] G. Oliva, R. Setola, and S. Panzieri. Distributed consensus under ambiguous information. *International Journal of Systems of Systems Engineering (IJSSE)*, 4(1):55–78, 2013.
- [62] Inter-Agency Task Force on Climate Change and Disaster Risk Reduction. Disaster risk reduction tools and methods for climate change adaptation. Technical report, UNISDR, 2010.

- [63] OTA (Office of Technology Assessment). *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage*. U.S. Government Printing Office, 1990.
- [64] Min Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121(0):43 – 60, 2014. ISSN 0951-8320. doi: <http://dx.doi.org/10.1016/j.res.2013.06.040>. URL <http://www.sciencedirect.com/science/article/pii/S0951832013002056>.
- [65] I. Patterson, J. Nutaro, G. Allgood, T. Kuruganti, and D. Fugate. Optimizing investments in cyber-security for critical infrastructure. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, CSIIRW '13*, pages 20:1–20:4, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-1687-3.
- [66] N. Petrovic, D. L. Alderson, and J. M. Carlson. Dynamic resource allocation in disaster response: Tradeoffs in wildfire suppression. *PLoS ONE*, 7(4):e33285, 04 2012. doi: 10.1371/journal.pone.0033285.
- [67] K. Poljansek, F. Bono, and E. Gutierrez. Seismic risk assessment of interdependent critical infrastructure systems: The case of european gas and electricity networks. *Earthquake Engineering & Structural Dynamics*, 41(1):61–79, 2012. ISSN 1096-9845. doi: 10.1002/eqe.1118. URL <http://dx.doi.org/10.1002/eqe.1118>.
- [68] M. Pollino, G. Fattoruso, A. B. Della Rocca, L. La Porta, S. Curzio, A. Arolchi, V. James, and C. Pascale. An open source gis system for earthquake early warning and post-event emergency management. In B. Murgante, O. Gervasi, A. Iglesias, D. Taniar, and B. O. Apduhan, editors, *Computational Science and Its Applications - ICCSA 2011*, volume 6783 of *Lecture Notes in Computer Science*, pages 376–391. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-21886-6. doi: 10.1007/978-3-642-21887-3_30. URL http://dx.doi.org/10.1007/978-3-642-21887-3_30.
- [69] M. Pollino, G. Fattoruso, L. La Porta, A. B. Della Rocca, and V. James. Collaborative open source geospatial tools and maps supporting the response planning to disastrous earthquake events. *Future Internet*, 4(2):451–468, 2012. ISSN 1999-5903.
- [70] C. Queiroz, A. Mahmood, Jiankun Hu, Z. Tari, and Xinghuo Yu. Building a SCADA Security Testbed. In *Network and System Security, 2009. NSS '09. Third International Conference on*, pages 357–364, Oct 2009. doi: 10.1109/NSS.2009.82.
- [71] Endsley Mica R. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37:32–64(33), March 1995. doi: doi:

- 10.1518/001872095779049543. URL <http://www.ingentaconnect.com/content/hfes/hf/1995/00000037/00000001/art00004>.
- [72] H. A. Rahman, M. Armstrong, DeTao Mao, and Jose R. Marti. I2sim: A matrix-partition based framework for critical infrastructure interdependencies simulation. In *Electric Power Conference, 2008. EPEC 2008. IEEE Canada*, pages 1–8, Oct 2008. doi: 10.1109/EPC.2008.4763353.
- [73] S. M. Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 2 - Volume 2*, HICSS '04, pages 20054.1–, Washington, DC, USA, 2004. IEEE Computer Society. ISBN 0-7695-2056-1. URL <http://dl.acm.org/citation.cfm?id=962750.962881>.
- [74] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21(6):11–25, Dec 2001. ISSN 1066-033X. doi: 10.1109/37.969131.
- [75] A. Rose and S.-Y. Liao. Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science*, 45(1):75–112, 2005. URL <http://www.scopus.com/inward/record.url?eid=2-s2.0-14744293206&partnerID=40&md5=7cdebaa34b610bb90b4218922dfa4d50>. cited By 141.
- [76] L. A. Rossman. *Computer Models/EPANET*. Water Distribution Systems Handbook. McGraw-Hill companies, 1999. ISBN 9780387372327.
- [77] De Porcellinis S., L. Issacharoff, S. Meloni, Rosato V., Setola R., and Tiriticco F. Modelling interdependent infrastructures using interacting dynamical models. *Int. J. Critical Infrastructure (IJCI)*, 4 (1/2):63–79, 2008. doi: 10.1504/IJCIS.2008.016092. critical infrastructures, CIP.
- [78] N. Santella, L. J. Steinberg, and K. Parks. Decision making for extreme events: Modeling critical infrastructure interdependencies to aid mitigation and response planning. *Review of Policy Research*, 26(4):409–422, 2009. ISSN 1541-1338. doi: 10.1111/j.1541-1338.2009.00392.x. URL <http://dx.doi.org/10.1111/j.1541-1338.2009.00392.x>.
- [79] G. Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, Princeton, 1976.
- [80] P. Smets and R. Kennes. The Transferable Belief Model. In RolandR. Yager and Liping Liu, editors, *Classic Works of the*

- Dempster-Shafer Theory of Belief Functions*, volume 219 of *Studies in Fuzziness and Soft Computing*, pages 693–736. Springer Berlin Heidelberg, 2008. ISBN 978-3-540-25381-5. doi: 10.1007/978-3-540-44792-4_28. URL http://dx.doi.org/10.1007/978-3-540-44792-4_28.
- [81] P. Sousa, A.N. Bessani, W.S. Dantas, F. Souto, M. Correia, and N.F. Neves. Intrusion-tolerant self-healing devices for critical infrastructure protection. In *Dependable Systems Networks, 2009. DSN 09. IEEE/IFIP International Conference on*, pages 217–222, June 2009. doi: 10.1109/DSN.2009.5270333.
- [82] S. Sultana and C. Chen. Modeling flood induced interdependencies among hydroelectricity generating infrastructures. *Journal of Environmental Management*, 90(11):3272 – 3282, 2009. ISSN 0301-4797. doi: <http://dx.doi.org/10.1016/j.jenvman.2009.05.019>. URL <http://www.sciencedirect.com/science/article/pii/S0301479709001534>.
- [83] D. Sutton, J. Harrison, S. Bologna, and V. Rosato. The contribution of neisas to ep3r. In Sandro Bologna, Bernhard Hammerli, Dimitris Gritzalis, and Stephen Wolthusen, editors, *Critical Information Infrastructure Security*, volume 6983 of *Lecture Notes in Computer Science*, pages 175–186. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-41475-6. doi: 10.1007/978-3-642-41476-3_15. URL http://dx.doi.org/10.1007/978-3-642-41476-3_15.
- [84] Stelios C.A. Thomopoulos. Sensor integration and data fusion. volume 1198, pages 178–191, 1989. URL <http://www.scopus.com/inward/record.url?eid=2-s2.0-0024818932&partnerID=40&md5=4218bcc0853e167b417e1628491a61f8>. cited By 7.
- [85] J. Timonen, S. Puuska, L. Laaperi, J. Vankka, and L. Rummukainen. Situational awareness and information collection from critical infrastructure. In *Cyber Conflict (CyCon 2014), 2014 6th International Conference On*, pages 157–173, June 2014. doi: 10.1109/CYCON.2014.6916401.
- [86] S. Tisue and Wilensky. Netlogo: A simple environment for modeling complexity. In *Int. Conf. on Complex Systems*, volume 5, 2004.
- [87] E. Todini and S. Pilati. Computer applications in water supply: Vol. 1—systems analysis and simulation. chapter A Gradient Algorithm for the Analysis of Pipe Networks, pages 1–20. Research Studies Press Ltd., Taunton, UK, UK, 1988. ISBN 0-471-91783-4. URL <http://dl.acm.org/citation.cfm?id=61052.61053>.
- [88] I.B. Utne, P. Hokstad, and J. Vatn. A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety*, 96(6):671 – 678, 2011.

- ISSN 0951-8320. doi: <http://dx.doi.org/10.1016/j.res.2010.12.006>. URL <http://www.sciencedirect.com/science/article/pii/S0951832010002620>. {ESREL} 2009 Special Issue.
- [89] M. van Eeten, A. Nieuwenhuijs, E. Luijff, M. Klaver, and E. Cruz. The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. *Public Administration*, 89(2):381–400, 2011. ISSN 1467-9299. doi: [10.1111/j.1467-9299.2011.01926.x](https://doi.org/10.1111/j.1467-9299.2011.01926.x). URL <http://dx.doi.org/10.1111/j.1467-9299.2011.01926.x>.
- [90] A. Varga and R. Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, Simutools '08*, pages 60:1–60:10, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). ISBN 978-963-9799-20-2. URL <http://dl.acm.org/citation.cfm?id=1416222.1416290>.
- [91] R.T. Watson. Synthesis report: A contribution of working groups i, ii, and iii to the third assessment report. Technical report, Intergovernmental Panel for Climate Change (IPCC), 2010.
- [92] F. E. White. Data Fusion Lexicon, Joint Directors of Laboratories. Technical report, Naval Ocean Systems Center, 1987.
- [93] L.A. Zadeh. *On the Validity of Dempster's Rule of Combination of Evidence*. Memorandum UCB/ERL-M. Electronics Research Laboratory, University of California, 1979.
- [94] L.A. Zadeh. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, 100, Supplement 1(0):9 – 34, 1999. ISSN 0165-0114. doi: [http://dx.doi.org/10.1016/S0165-0114\(99\)80004-9](http://dx.doi.org/10.1016/S0165-0114(99)80004-9). URL <http://www.sciencedirect.com/science/article/pii/S0165011499800049>.
- [95] R. Zanjirani Farahani, N. Asgari, N. Heidari, M. Hosseini, and M. Goh. Covering problems in facility location: A review. *Computers & Industrial Engineering*, 62(1):368 – 407, 2012. ISSN 0360-8352. doi: <http://dx.doi.org/10.1016/j.cie.2011.08.020>. URL <http://www.sciencedirect.com/science/article/pii/S036083521100249X>.
- [96] B. Zhu, A. Joseph, and S. Sastry. A taxonomy of cyber attacks on scada systems. In *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ITHINGSCPCOM '11*, pages 380–388, Washington, DC, USA, 2011. IEEE Computer Society. ISBN

978-0-7695-4580-6. doi: 10.1109/iThings/CPSCCom.2011.34. URL <http://dx.doi.org/10.1109/iThings/CPSCCom.2011.34>.

- [97] R. Zimmerman. Decision-making and the vulnerability of interdependent critical infrastructure. In *Systems, Man and Cybernetics, 2004 IEEE International Conference on*, volume 5, pages 4059–4063, 2004. doi: 10.1109/ICSMC.2004.1401166.

PUBLICATIONS

JOURNALS

- [JDPGP¹⁵] A. Di Pietro, A. Gasparri, and S. Panzieri. Distributed data fusion for situation awareness in critical infrastructures with link failures. *International Journal on Critical Infrastructure Protection*, 2015. Submitted.
- [JDPLP⁺₁₅] A. Di Pietro, L. Lavallo, M. Pollino, A., V. Rosato, and A. Tofani. Supporting decision makers in crisis scenarios involving interdependent physical systems. *International Journal of Disaster Risk Reduction*, 2015. Manuscript in Preparation.
- [JPP₁₄] A. Di Pietro and S. Panzieri. Taxonomy of SCADA systems security testbeds. *Int. Journal of Critical Infrastructures*, 10(3):288–306, January 2014.
- [JTSDP⁺₁₅] A. Tofani, Alessandroni S., A. Di Pietro, L. Lavallo, M. Pollino, A., and V. Rosato. CIPRNet decision support system: Modelling electrical distribution grid internal dependencies. *Journal of the Polish Society of Safety and Reliability*, 2015. Submitted.

BOOK CHAPTERS

- [BFDPA⁺₁₄] V. Formicola, A. Di Pietro, A. Alsubaie, S. D’Antonio, and J. Marti. Assessing the impact of cyber attacks on wireless sensor nodes that monitor interdependent physical systems. In Jonathan Butts and Sujeet Sheno, editors, *Critical Infrastructure Protection VIII*, volume 441 of *IFIP Advances in Information and Communication Technology*, pages 213–229. Springer Berlin Heidelberg, 2014.

PROCEEDINGS

- [SAADP⁺₁₄] A. Alsubaie, K. Alutaibi, A. Di Pietro, J. R. Marti, and A. Tofani. Resources allocation in disaster response using ordinal optimization based approach. In *IEEE Canada International Humanitarian Technology Conference (IHTC)*, 2014.
- [S₁₁] A. Alsubaie, A. Di Pietro, J. Marti, P. Kini, Ting Fu Lin, S. Palmieri, and A. Tofani. A platform for disaster response planning with interdependency simulation

- functionality. In *Critical Infrastructure Protection VII - 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers*, pages 183–197, 2013.
- [SBHB⁺₁₄] A. Burzel, M. Hounjet, B. Becker, A. Di Pietro, M. Pollino, V. Rosato, and A. Tofani. Toward a decision support system for consequence analysis of flooding on critical infrastructure. In *11th Int. Conf. on Hydroinformatics (HIC 2014)*, 2014.
- [SDPFPP₁₃] A. Di Pietro, C. Foglietta, S. Palmieri, and S. Panzieri. Assessing the impact of cyber attacks on interdependent physical systems. In *Critical Infrastructure Protection VII - 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers*, pages 215–227, 2013.
- [SDPGP₁₅] A. Di Pietro, A. Gasparri, and S. Panzieri. Situational awareness in critical infrastructures using distributed information fusion with evidence discounting. In *Critical Infrastructure Protection VIII - 8th IFIP WG 11.10 International Conference, ICCIP 2013, Arlington, Virginia, USA, March 16-18, 2015, Revised Selected Papers*, 2015. To appear.
- [S55] J. R. Marti, P. Kini, P. Lusina, A. Di Pietro, B. Charnier V. Rosato and, and K. Wang. Inter-system software adapter for decision support by interfacing disaster response platforms and simulation platforms. In *Global Humanitarian Technology Conference (GHTC), 2012 IEEE*, pages 41–46, Oct 2012.
- [SRDPL⁺₁₄] V. Rosato, A. Di Pietro, L. La Porta, M. Pollino, A. Tofani, J. R. Marti, and C. Romani. A decision support system for emergency management of critical infrastructures subjected to natural hazards. In *9th Int. Conf. on Critical Information Infrastructure Security (CRITIS 2014)*, 2014.
- [SRPA⁺₁₂] V. Rosato, A. Di Pietro, G. Aprea, R. Delfanti, L. La Porta, J. R. Marti, P. Lusina, and M. Pollino. Interaction between environmental and technological systems: toward an unifying approach for risk prediction. In *7th Int. Conf. on Critical Information Infrastructure Security (CRITIS 2012)*, 2012.