Chiara Foglietta

SYSTEM METHODOLOGIES FOR SITUATION AWARENESS AND RISK MANAGEMENT FOR CRITICAL INFRASTRUCTURE PROTECTION

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

XXV Cycle

SYSTEM METHODOLOGIES FOR SITUATION AWARENESS AND RISK MANAGEMENT FOR CRITICAL INFRASTRUCTURE PROTECTION

Ph. D. Student: Chiara Foglietta Signature: _____

Advisor: Stefano Panzieri Signature: _____

Course Coordinator: Stefano Panzieri Signature: _____

February 2013

System Methodologies for Situation Awareness and Risk Management for Critical Infrastructure Protection

A Thesis presented by
Chiara Foglietta
in partial fulfilment of the requirements for the degree of
Doctor of Philosophy
in Computer Science and Automation
Dept. of Engineering

University of "Roma TRE"

February 2013

I known the price of success: dedication, hard work,
and an unremitting devotion to the things you want to see happen.

— Frank Lloyd Wright

Dedicated to my dad.

ABSTRACT

The Mixed Holistic Reductionist Approach is a methodology that merges the holistic and the reductionist techniques trying to conserve the pros. The aim is the modelling of critical infrastructure interdependencies and the assessment of impact due to physical failures and to cyber threats. This approach can be applied both in distributed and in centralised contexts. The distributed framework is mandatory if the communication among control centres is peer-to-peer.

In order to manage also cyber threats, Situation Awareness models and techniques help in order to classify faults and failures. In fact, Data Fusion methodologies, as Evidence Theory, can detect the most probable cause of faults happened in facilities and, therefore, we uses the other information, coming from Evidence Theory results, as another input for the MHR approach.

The state estimation is one of the key functions of SCADA systems for grids. In order to identify the state of the system, state estimation helps in accurate and efficient monitoring of operational constraints. The ability to provide a reliable state can also help in contingency analyses and in the required corrective actions. The smart grid context is quite different respect to traditional distribution grid, starting from different topology features, so a new approach to state estimation is mandatory.

ACKNOWLEDGMENTS

It would not have been possible to write this doctoral thesis without the help, support and patience of the kind person around me, to only some of whom it is possible to give particular mention here.

This thesis would not have been possible without the presence, help, support and patience of my supervisor, Prof. Stefano Panzieri. He is able to help me and understand my "bad" moments. I also thank Prof. Stephen D. Wolthusen for inviting me in his working group, for supporting me during the stay in Egham at the Royal Holloway University of London.

I would like to thank Vincenza "Cinzia" Abate for her kindness, friendship and support, together with the other Ph.D students of the XXV cycle, especially Attilio Priolo, without him the first two years has been a dark hole. The older Ph.D students, as Gabriele Oliva and Sandro Meloni, have been a guide to understand the mechanisms and the tricks in the research and university world. The younger Ph.D students, as Simone Palmieri, Antonio Di Pietro and Jagadeesh Gunda, have the same enthusiastic energy to stimulate me towards new goals and objectives.

A special thank goes to Riccardo Santini, "my" best master thesis student. In the last more than three years, I see a lot of students doing their best to obtain their degree, but seeing someone so enthusiastic and hard-headed is always a pleasure to work with. With him and Giovanni Corbò, the M·CIP lab is completed.

I would like to thank all the Egham boys and girls, i.e., Alessio Baiocco, Yangue "Yaya" Feng and Cristina Alcaraz. Those moments spent with them are a gift for me.

I am also grateful to all the secretaries of the Computer Science and Automation Department, for their help and support, for their patience in my messes and noises, and for their constant understanding.

Thanks to Alessandro Longhi, my neighbour in the Robotic Laboratory. He is the supporter of my messes, my songs, and my noises. The cappuccino moments are the best instants in the day. I'm very sorry for all the troubles that I always create to you.

Last, but not least, my family: Adele, Ilaria and Diana, my personal big-dog. The last three years were often not happy, but all the moments we lived together tied and enriched us.

For any errors or inadequacies that may remain in this work, of course, the responsibility is entirely my own.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Industrial control system (ICS) is a general term that encompasses several types of control systems, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and Critical Infrastructures.

Industrial control systems and critical infrastructures' control centers are able to collect a large amount of data and to elaborate such an information in order to provide the operators with a synoptic view of the ongoing situation. The operator, on the base of such information, is able to understand the ongoing situation and undertake his decisions. Such a paradigm, although effective when infrastructures are relatively decoupled, is becoming less and less adequate derived from the increasing degree of dependency and interoperability among infrastructures. Interdependency arises for many reasons and, in particular, because of geographical, physical, cyber, or logic relations [77].

Helping operator in decisions is one of objective of critical infrastructure research. The operator panels are an efficient way to display other important information, coming from other interconnected infrastructures. The data exchange among control centre must be executed in a secure way, but also using partial information. In the Chapter 1, the information is combined at service layer and it is another kind of encryption.

Cyber interdependency, in particular, is becoming more and more pervasive, due to the increasingly use of internet-based technologies and public networks to operate Critical Infrastructures. However, while the Internet has been beneficial to both public and private organizations, the increasing reliance on networked systems has augmented the risk of cyber attacks.

SCADA (Supervisory Control and Data Acquisition) systems, first introduced in the 80's and 90's, are still in use. These systems, including those installed until few years ago, did not consider properly the

security issues due to the usage of public networks. Such systems were conceived with a monolithic structure, isolated from the outside world and based on proprietary standards for the communication between control center and field devices.

Over time, due to the rapid growth of the Internet and telecommunications networks, SCADA systems have changed, slowly tending to a distributed architecture, with standardized and well documented communication protocols, such as TCP/IP and Modbus. These SCADA systems are usually connected to Corporate Network. In addition, such systems typically exchange data with no encryption or authentication algorithms.

However, in recent years, there is a growing urge to evaluate the performances of SCADA systems also from the point of view of security. This need arises due the great relevance of these systems for the welfare of citizens and nations. In 2010, the discovery of Stuxnet [33] became a concrete proof that cyber attacks on industrial control systems and SCADA systems are possible. Stuxnet was able to infect Windows computers used to supervise industrial control systems, and to recognize and infect such control systems. In 2010 and in 2011, the amount of SCADA vulnerability disclosures and exploits has exploded. Terry McCorkle and Billy Rios found 100 SCADA bugs in 100 days, thanks to free software available on-line [79].

Impact evaluation of cyber attacks and their consequences are very difficult to perform. The complexity of the problem at hand is indeed non-trivial also due to interdependencies. In fact the domino and cascading effects are sometimes not easy to find, especially with due to the growing importance of telecommunications that may result in unwanted and unnoticed couplings.

For the above reasons, the impact assessment of faults should also encompass cyber attacks, which are becoming a realistic typology of attack for Critical Infrastructures. The introduction of firewalls, intrusion detection systems (IDS) and degrees of separation between the Corporate Network and the control system network is a good step toward increasing security, but there is still much to be done. In Chapter 2 the evaluation of cyber attack impact is included in MHR approach.

Another step that may result in an increase of the resilience of facilities is the information exchange among governments and infrastructure owners. The information can be shared using national and international agencies, such as CERTs (Computer Emergency Response Teams), or early warning and alerting networks, as EISAC (European Information Sharing and Alert System), American National Cybersecurity and Communications Integration Center (NCCIC) or Australian Cyber Security Operations Centre (CSOC).

All the agencies listed above were created with the goal of cooperating with infrastructure operators in the event of a cyber attacks. Each infrastructure, upon suspicion of being under attack, warns its

agency or CERT that has the duty to share information with other agencies and infrastructures that may be involved. In addition, they provide mitigation mechanisms and countermeasures.

Evaluating cyber attack impact is a very important feature, but the natural evolution is the attempt to merge cyber and physical information in order to augment the Situation Awareness. For this reason, the model and methodologies in the Data Fusion context have been analyses in Chapter 3.

Evidence Theory is the focuses of Chapters 4 and 5 with its enhancement. First of all, it has been applied the Evidence Theory framework in distributed conditions, with the application of networked Transferable Belief Model in the Critical Infrastructure domain. The other field is related to the knowledge model and the ability of Evidence Theory to change ideas thanks to evolving situations.

Among Critical Infrastructures, great importance is the energy sector and especially the power generation, transmission and distribution. The role of electric power systems has grown steadily in both scope and importance with time, and electricity is increasingly recognized as a key to societal and economic progress in many developing country.

Since the fast advancement of computer and communication technologies in the late 1980s, there has been a trend to optimize and control power system in a distributed or hierarchical manner. In the day to day operation and control of large-scale electric power systems, operators depend on a measured quantities, such as bus voltage magnitudes, line flows, and bus loads and injections, in order to monitor the present status of the grid and to initiate control actions. Because the data acquisition process involves a number of complex procedures, the measurements contain errors. The goal of power system state estimation is to provide reliable, accurate and complete set of data for real-time monitoring and control of power systems. In Chapter 6, hierarchical power state estimation is proposed and analysed in order to apply it in smart grids. Further analyses are currently under investigation for data injection attacks in the hierarchical model, in order to understand the differences with the classical model.

The thesis is organized in three major clusters: Chapters 1 and 2 deal with Critical Infrastructures modelling and impact assessment of faults and failures; in Chapters 3, 4 and 5, Situation Awareness problem is described and Evidence Theory is applied to impact assessment of cyber and physical damages to interconnected complex systems; in Chapter 6 the State Estimation module in Energy Management Systems is described with a hierarchical structure; conclusions and future works are in Chapter **??**.

1

MODELLING INTERDEPENDENCIES IN DISTRIBUTED CONTEXT

In the literature many approaches have been proposed to represent interdependency among Critical Infrastructures and their elements; these models, however, are mostly used off-line for simulations and impact analysis.

In this Chapter, an interdependencies modelling is proposed, called Mixed Holistic Reductionist (MHR) Approach, able to evaluate impact assessment and manage risk. This model allows combining the holistic method with the reductionist, trying to maintain the benefits of both paradigms. Another feature is the assessment of services towards customers and other operators. In fact, stakeholders and operators are focused on services and their quality for contract reasons.

This approach has been implemented using an agent-based simulator, CISIA (Critical Infrastructure Simulator by Interdependent Agent) developed by "Roma TRE" University.

The research innovation is the validation phase of our approach in real and distributed context. In fact, this methodology has been developed for impact assessment in distributed and on-line context, where partial observations are composed into a wider perspective by exchanging only very abstract information, such as the quality of services. The main advantage of such a system is that the operators of the different infrastructures are able to make better decisions, because they are aware of the actual and foreseen unavailability of the services provided by the other infrastructures.

Moreover, due to the structural lack of adequate quantitative data, the interdependency model adopted is based on fuzzy numbers, and is tune-able with linguistic information obtained by stakeholders and experts of the different infrastructures.

The tool has been implemented and tested with respect to a real case study and it has been designed in order to be easily scalable

and extensible, within two FP7 EU projects: MICIE project [1] and COCKPITCI [3].

1.1 STATE OF THE ART

It is a fact that infrastructures are becoming more and more complex, tightly interconnected and mutually dependent, according to many dimensions, such as geographic proximity, cyber connection (i.e., reachability via the web) or resource exchange dependencies [78].

The word "infrastructure" is the "basic, underlying framework or features of a system or organization" [2]. For the United States, the general definition of critical infrastructure in the overall US critical infrastructure plan is: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [65].

Indeed the problem is complex mainly due to the exponential relevance of web based technologies used to control the infrastructures, these systems are becoming more and more interoperable; conversely, due to their complexity, the knowledge of human technicians is becoming more and more sector-specific. The paradox is that, very often, Critical Infrastructures and their subsystems interact in ways that are hidden and not well understood by the single infrastructures' experts, while this interaction represents the main cause of coupling among these systems, often leading to cascading failures and domino effects. This is the reason why sector-specific simulators and monitoring systems, although being very sophisticated, fail to capture the behavior of the infrastructures in critical situations, when domino effects arise.

Modeling and simulation (M&S) tools for individual infrastructures are rather well developed today. Many commercial products are available that enable infrastructure owners to operate, and manage their systems, and to foresee their evolution. However, M&S tools for multiple, interdependent infrastructure are immature by comparison.

In the literature many approaches have been proposed to represent the complexity of interdependent critical infrastructures; these methods are, typically, adopted in order to perform "what if?" analyses and ex-post simulations, with the aim to understand structural vulnerabilities, to asses and mitigate the risk of domino effects and multiple disruptions and to provide a support to decision-makers.

In [78], the authors emphasize how dependency and interdependency should be analysed with respect to different dimensions. In particular they catalogue dependencies into four, not mutually exclusive, classes:

- *Physical Dependency.* Two infrastructures are physically dependent if the operations of one infrastructure depends on the physical output of the other.

- *Geographical Dependency*. A geographic dependency occurs when elements of multiple infrastructures are in close spatial proximity. In this case, particular events, such as an explosion or a fire in an element of an infrastructure may create a failure in one or more near infrastructures. This link is not generally accepted by all researchers, see for further information [64].

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

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

In order to obtain insight on the behavior of interdependent infrastructures, a first step is to consider a topological characterization of the infrastructures, representing them as complex networks composed of similar basic elements, inspecting emerging behaviors generated by the interconnection of such elements [99, 50, 80, 30].

In [53] a system composed by several homogeneous networks that interact exchanging loads is analysed; in [61] there is an attempt in the direction of studying heterogeneous interdependent networks (i.e., formed by infrastructures of different nature) showing that the coupling makes the system more susceptible to large failure. A similar result has been reported in [14] where statistical mechanical and mean field theory are used to extrapolate steady state solutions in response to removal of a fraction of nodes. In [91] there is an attempt to formalize the interdependent dynamics among several heterogeneous infrastructures, considering the interconnection between a power grid and the telephony network and inspecting the effect of node removal. A similar formalism has been proposed in [54] where five types of infrastructure interdependencies are presented and incorporated into a network flow framework and tested with reference to the lower Manhattan region of New York. In [80] the interconnection properties of an electric grid and a telecommunication network that mimic the Italian situation are studied, relying on the DC Power Flow Model [100] to represent the electric power flow and considering also the packet routing in the telecommunication network.

The assumption of homogeneity (i.e., the nodes represent entities of similar nature), however, limits the applicability of these methodologies, since in real cases infrastructures are composed of highly

heterogeneous subsystems; moreover topological methods typically limit their scope to the geographical interaction of subsystems.

A step further is done by adopting a simulative perspective, focusing on the representation of the isolated behavior of subsystems and then considering their interaction by means of simulation platforms and tools [73, 21, 73, 46]. The interested reader can refer to the survey conducted by Idaho National Laboratory [73].

Among the others, the Input-Output Inoperability Model (IIM) [48] gained large attention. The idea is that each infrastructure is characterized by an inoperability $q_i(t)$, that represents its percentage of malfunctioning, while $q(t)$ is the vector of inoperability of all the infrastructures; the infrastructures are then considered as linearly dependent according to the following equation

$$\dot{q}(t) = Aq(t) + c \tag{1}$$

where c is the induced perturbation and A is the Leontief matrix whose coefficients a_{ij} represent the coupling between the $i-th$ and $j-th$ infrastructure. Within this modelling framework, however, the interactions among different infrastructures are modelled with an high level of abstraction, while the behavior of the subsystems underlying the different infrastructures is masked; for instance it is possible to determine that an infrastructure is 50% inoperable, but it is not possible to distinguish whether half of the equipments of the infrastructure are down or the equipments' working condition is degraded. Another limitation of the IIM model its the economic origin; the main assumption of the model is in fact that the coupling among infrastructure is proportional to their economic interaction.

In [67] a first step has been done in order to overcome these limitations, decomposing the infrastructures into a set of components and subsystems and considering the exchange of resources among these subsystems, thus allowing to tune the model by means of information elicited by infrastructures' experts.

Such an idea has been further expanded in Agent Based approaches [82, 67], where infrastructures are decomposed into a set of interacting software agents, each with a dynamic behavior and with heterogeneous level of abstraction.

In order to enhance the comprehension of highly interdependent scenarios, in [24, 21] the agent-based perspective was further enriched, considering, at the same time, multiple and partly overlapping representations of the scenario (i.e., physical, functional and global representations).

As exposed above, limiting the scope to the interaction among subsystems may lead to crude approximations, in fact, besides being a set of interconnected components, an infrastructure is characterized by emerging functional behaviors and is greatly influenced by human

behavior and sociological phenomena. When dealing with complex, highly interdependent scenarios, a single perspective may be reductive, as stressed in [37].

An effective approach, then, is to take into account multiple representations of the same reality, each aimed to highlight a particular class of phenomena.

In [24] Critical Infrastructures are represented according to three hierarchical layers:

MICRO-LEVEL: represents the physical components that constitute the functional elements of an infrastructures (i.e., electrical equipments, gas valves, etc.)

MESO-LEVEL: represents an infrastructure network at the system level (i.e., network nodes and links, power generators and loads, etc.)

MACRO-LEVEL: represents the territory or zone which depend on the service provide by the infrastructure.

Within this framework, each level is considered as a nested subsystem, which can be analysed independently. Moreover, the propagation of effects is assumed to spread from the micro to the macro level, neglecting downstream consequences and focusing on the effect of outages and failures on higher levels.

1.2 MIXED HOLISTIC REDUCTIONIST APPROACH

Most of the modelling approaches discussed above focus on the overall, holistic, perspective or deeply inspect the cross-domain interactions among elementary, reductionist, elements.

In order to overcome these limits, we introduce a Mixed Holistic Reductionist approach (MHR) [21]. MHR approach is a methodology able to modelling interdependencies and Critical Infrastructures, respect to predefined level of quality to customers or other facilities. In such a perspective, the best aspects of both approaches are maintained: the interdependencies among elementary components are modelled with the reductionist method, and the relations at high level are modelled through the holistic vision.

MHR methodology contemplates infrastructure modelling at different hierarchical levels. The basic idea is to integrate three levels of abstractions, into a single simulator: holistic, reductionist and service.

Peculiarity of the MHR methodology is to combine pros of both the reductionist and the holistic approaches: interdependencies among elementary components are modelled with the reductionist method, and internal relationships, within the single facility, are modelled through the holistic view.

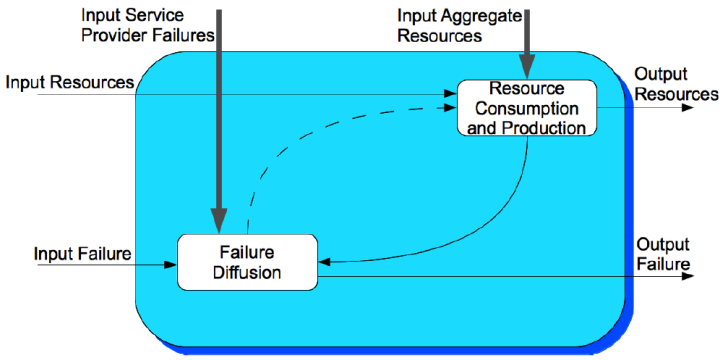

Figure 1: Reductionist entity representation

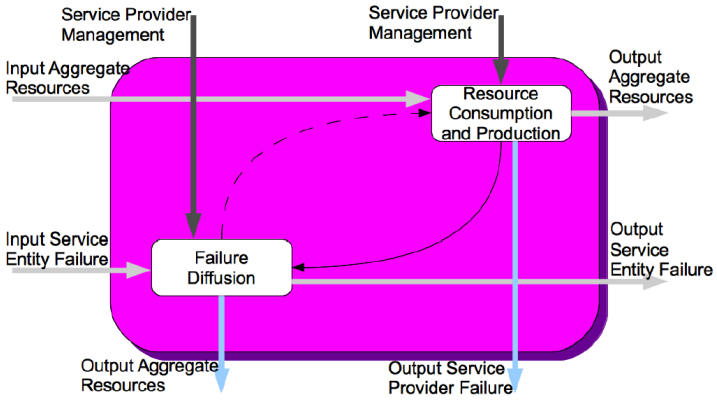

Figure 2: Service entity representation

Reductionist approach tries to model complex systems into smallest and simplest pieces. The holistic method reviews complex systems as the whole web of interactions. Both methods have benefits and drawbacks, so we want to apply the methodologies together, in order to overcome disadvantages of holistic and reductionist approaches. Between these two levels, an additional layer, called service layer, has been introduced to connect two opposite methodologies. This is a midway level of abstraction: this layer is necessary to focus particular services vital for customer satisfaction and to disaggregate resources and services from the holistic view into the reductionist equipment.

With a reductionist perspective (see Figure 1), each infrastructure is decomposed into a web of interconnected elementary entities (or blocks); these entities receive and generate resources and may propagate failures according to proximities of different nature; therefore, their behaviour depends by the (mutual or not) interactions with the other reductionist elements. Moreover, their capability to correctly operate depends also by the availability and quality of some aggregate resources (or services) provided by service layer.

Services are introduced as functional blocks (see Figure 2) demanded to provide specific, yet high level, functions to reductionist elements

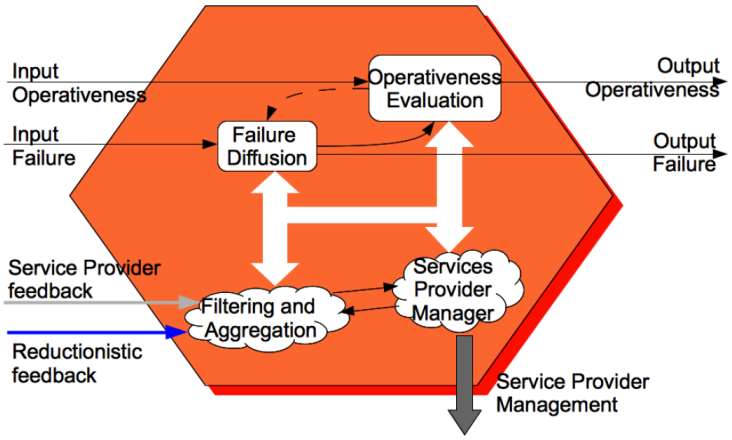

Figure 3: Holistic entity representation

belonging to the same or different infrastructure. Analogously to reductionist elements, services require and provide (aggregate) resources and may suffer and propagate some failures; this allows to model complex and high-level failures (e.g. the effects of cyber attacks) that, instead, are very complex to model with a mere reductionist perspective. The operativeness of each service is largely influenced by the operative condition of the infrastructures, and by the policies and management strategies adopted in the specific context by the infrastructure's stakeholders.

Holistic blocks represent the holistic view of the infrastructures (see Figure 3), and they interact with other holistic entities exchanging their operativeness. In this case the failure block allows modelling specifically some events like malicious behaviors, that should be very difficult to model at different abstraction levels. Holistic blocks have the duty to influence the operative conditions of service layer on the base of the feedbacks received from reductionist elements and considering also the overall status of the infrastructure itself. Moreover every holistic node must provide adequate management service to service layer, by means of the definition and execution of adequate control actions (i.e., flow redirections, parameter configuration, event-driven suspension/reactivation/recovery, etc ...) in order to react to adverse events which may cause a degradation or denial of the aggregate resources provided by service layer and generate cascading propagation of faults.

Finally, an holistic node must be aware of the operativeness of its own service layer, in order to obtain a complete knowledge of the status of the infrastructure itself and then update the overall operativeness accordingly. In Figure 4 an example of the elements used inside the model is reported; in this case there are two infrastructures, electrical power distribution (ELE) and telecommunications (TLC), that are interdependent at every level.

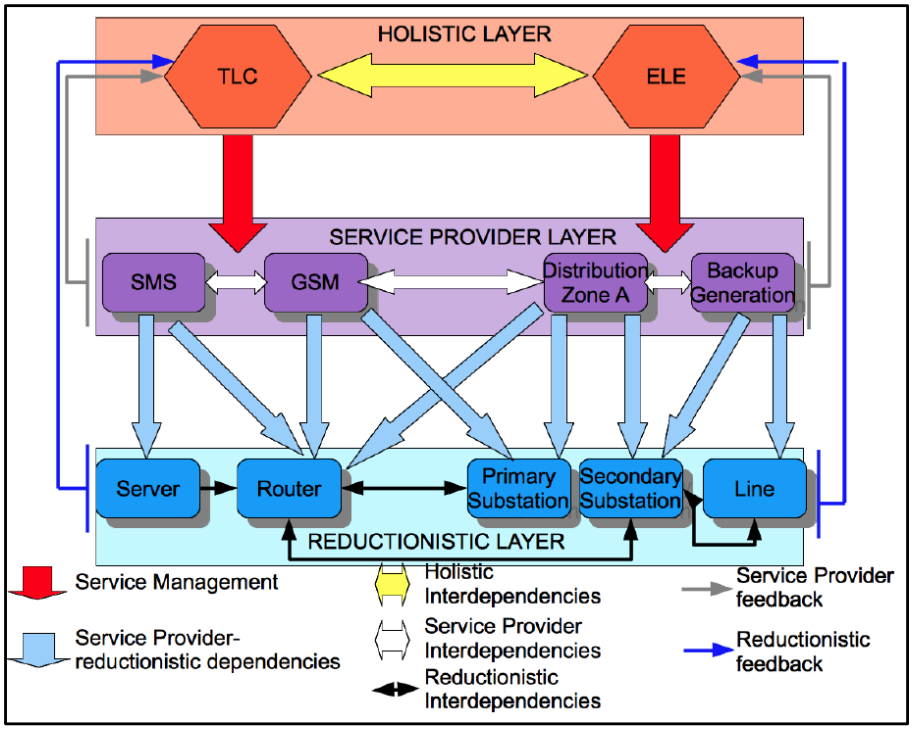

Figure 4: A graphical representation of an application for MHR approach

In Figure 4, an application of this approach is depicted, using the CISIA software. We consider two infrastructures interdependent between each others: telecommunication network and power grid. Initially we described the two infrastructures as a unique agents at holistic layer. In the service provider layer, we choose services that are necessary to describe the Quality of Service (QoS) to customers: in telecommunication network services can be SMS and GSM, instead for the power grid the services are the ability to fed customer with distribution network and backup power distribution. At service provider layer, interdependencies are detailed respect to considered services. The interconnections between service of the same facility are always known to operators, instead the interconnections among different infrastructures are more complex. In this case, GSM equipment are fed by the distribution service in zone A and the backup distribution is always ordered by SCADA control center using telecommunication services. Reductionist layer explains a more detailed level of abstraction, usually considering the equipments. Interdependencies are described by links among instruments, as the interconnections between power substations and telecommunication routers.

In Figure 4 are also depicted feedback from reductionist and service layers into holistic layer, as usually happens in control loop, to report faults and alarms. The presence of feedback arrows is not mandatory and it is usually applied to send "broadcast" information about faults and failures. Data, coming from SCADA systems, are related

to reductionist agents (i.e., short-circuit at load level), then they influence holistic nodes and, therefore, services. Due to feedback loops and all possible connections among layers, the distributed approach can be applied. In fact, the transmitted data between control centres is just the one related to services and holistic agents, in order to preserve the privacy of the real data in the fields. So services and holistic nodes must affect in some ways also the reductionist equipment.

Notice that, although being a very flexible and powerful formalism, the main drawback of such a methodology is that the effort required to tune the model is directly proportional to the degree of detail required. Nevertheless, this is a common problem of knowledge and system modelling.

A relevant issue is how to reverse the (mono-directional) dependencies between services and reductionist elements; in fact, specifying the exact contribution exerted by each single reductionist element on the different services may lead to unmanageable complexity. Indeed such inverse dependencies are mostly hidden and complex from the point of view of the single service; moreover usually the adequate control actions performed in order to grant an acceptable quality of such services are demanded to entities with a wider perspective (i.e., a control room). Hence it is more rational that an service relays on data provided by a management entity with an overall vision, able to filter the huge amount of reductionist data, instead of taking into account the contribute of every single component.

Notice that, in the proposed framework, services are not directly dependent on the reductionist elements, but are dependent on aggregate information coming from higher level nodes, which have a wider perspective.

1.3 CRITICAL INFRASTRUCTURE SIMULATION BY INTERDEPENDENT AGENT (CISIA)

Based on the MHR approach, in this section, the Critical Infrastructure Simulation by Interdependent Agent (CISIA) [21] framework will be detailed where connections among entities, including in different layers , and the transmission mechanisms are described. CISIA is an agent-based interdependency modeling framework. The overall system of system is decomposed into a set of n entities, and the spreading mechanisms of m resource typologies and k classes of failure are considered.

Such framework considers multiple interconnection matrices, which represent the different typologies of interaction; the result is a multigraph, which allows performing complex topological and dynamical analyses.

Within this approach, all the elements follow a common general model:

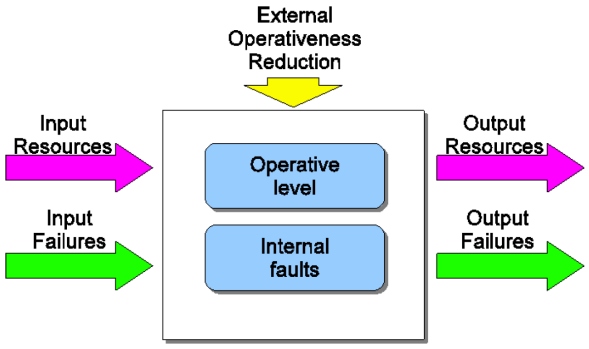

Figure 5: Input-output CISIA entity behavior

- Elements exist in order to produce, and transport or consume tangible or intangible resources (goods, services, policies, management, etc);
- Elements may suffer faults or failures;
- Different faults may be propagated, or propagate their negative effects, according to proximities of different nature;
- The capability of each element 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 affect it.

Each CISIA entity can be represented as in Figure 5 through an input/output behaviour. The operative level is a quantity which summarizes the status of the entities, and which is used to drive the behavior of such elements. Each entity receives some input resources and some input failures, and generates output resources and failures.

The model is able to take into account an external operativeness reduction, in order to represent the disruptive phenomena which may cause the inoperability of an element. CISIA entity are then interconnected by means of different adjacency matrices, whose links are characterized by an attenuation, due to dissipation phenomena, and a time delay.

Moreover, in order to effectively represent the uncertainty of human operators and actors, all the variables describing the dynamics of entities are expressed by Fuzzy numbers (FN) [29]. Fuzzy numbers can be seen the most natural way to introduce model and data uncertainty in a technical talk.

The implementation of CISIA has been performed in ANSI C++, strictly following an object oriented approach.

In Figure 6 we describe the basic input-output characteristics of a generic element; such a block is composed by a set of N input (or output) ports, each demanded to send or receive some resources or

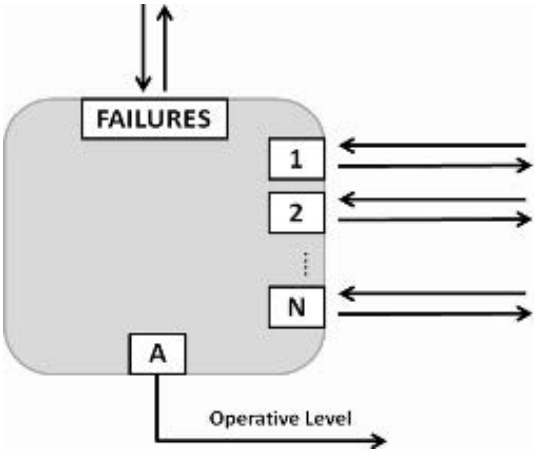

Figure 6: Representation of generic CISIA entity ports

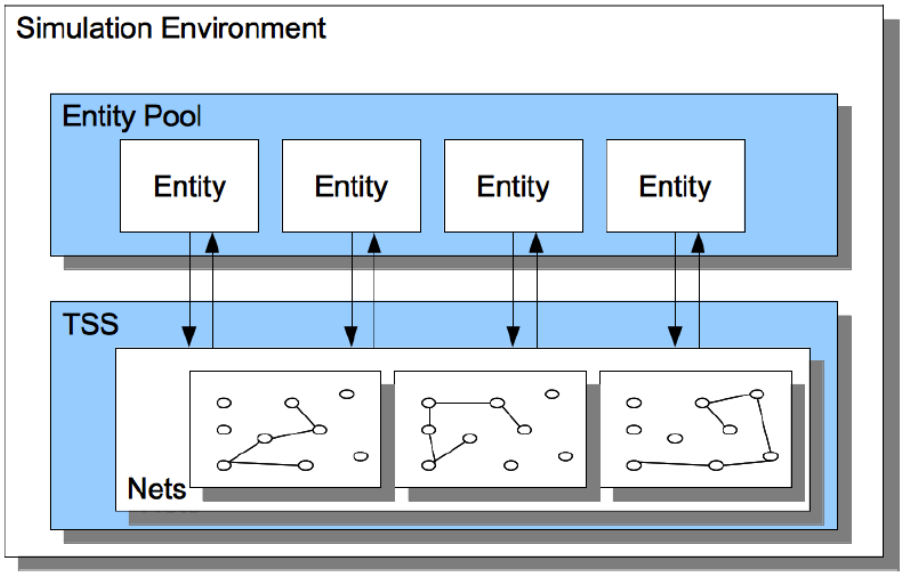

Figure 7: The structure of CISIA simulator

failures. Within such a general model, many configurations are possible; however every element is at least equipped with a "failure" port devoted to send (or receive) failures and an port, called "A" used to forward its operative level.

Within the simulator, a simulation instance is primarily constituted by the entities and the adjacency matrices that interconnect them; in fact there is the possibility to specify, at every abstraction level, multiple graphs, each describing the exchange of a particular resource or the diffusion of a particular class of failure (i.e. geographic, cyber, sociological, etc.). Entities and matrices are collected in two main structures, respectively Entity Pool (EP) and Transmission Sub System (TSS), both depicted in Figure 7.

Each simulation step is driven by the clock, a routine that synchronizes the computation steps of the entities with the message exchang-

ing phase, managed by the TSS; at each step entities generate their resources and failures and such quantities are routed to other elements according to the multi-scale, multi-graph topology of the framework. Each link can be equipped with a defined delay in terms of time steps required for the transmission of the resource/failure, and with an attenuation that represents a dissipation or attenuation of the quantity during the transmission.

Moreover each timed cycle begins with a set of instantaneous cycles, in order to depict real-time dependencies; in fact it is not possible that an element within a power grid has to wait some cycles to receive power, such a resource has to be instantly forwarded (and the lack of such a resource has to be instantly noticed). Therefore at the beginning of every timed cycle many instant cycles are performed, until the overall system reaches a steady state.

As shown in Figure 7, the Transmission Sub System (TSS) is devoted to manage the communication between the entities. The TSS stores the matrices which describe the different types of adjacency between the entities, as exposed above. Entities communicate via message exchanging, where each message contains data about the type and the denormalized quantity of carried resource (or fault), the normalizing factor, unit of measurement and the sender port identification (ID). When the TSS receives the signal from the simulation clock, it collects the outgoing messages from all the entities and delivers each message to the neighbours of the sender entity, according to the adjacencies described in the matrix associated with the type of the carried quantity. If a link between two adjacent entities is characterized by attenuation or delay factors, TSS provides to delay the delivery of the messages routed over that link and to suitable scale the carried quantities.

The Entity Pool (EP) synchronizes the execution steps of the entities and to manage their persistence. EP stores the entities inside a multi indexed vector, keeping also the map between the communication ports and the correspondent entities. When it receives a signal from the simulation clock it keeps the execution control, and spanning the vector which contains the entities, launches the atomistic simulation step on each entity. Once all the entities have run their simulation steps, gives back the control to the clock. After this step the EP waits for the execution of the communication phase, exploited by the TSS. During this phase it works as a mapping interface between the calls of the TSS and the communication routines of the entities.

The CISIA framework, therefore, is a discrete-time, agent-based methodology able to represent the exchange of resources and failures among the entities, considering also the attenuations and delays which may occur during transmission.

Moreover, the interdependency is modelled by means of multiple adjacency matrices, resulting in a multi-graph. Finally, each quantity

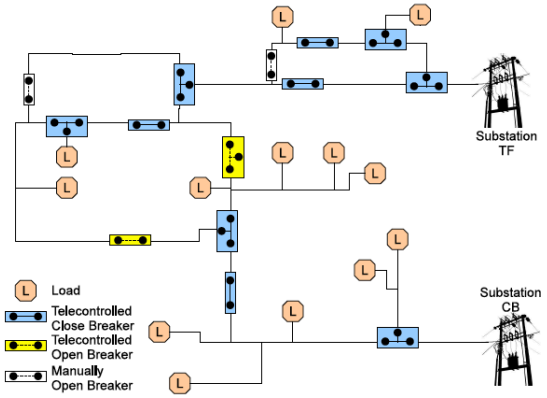

Figure 8: The considered MV power grid

is modelled by means of Triangular Fuzzy Numbers [29], allowing to encode vague information and providing an estimation of the certainty of the simulation/prediction.

1.4 EXAMPLE OF INTERDEPENDENT CRITICAL INFRASTRUCTURES

In this section we describe an example of the infrastructures considered in the case study will be outlined, then some results will be provided. However, due to non disclosure issues, the numerical results of this section are very general and are aimed to demonstrate the potentialities of the approach (see the MICIE website [1] for more details).

The infrastructures considered in the case study are:

1. A portion of a Medium Voltage (MV) power distribution grid;
2. A SCADA system that controls the grid, allowing the communication among SCADA centers and Remote terminal units (RTUs) that physically operate the network;
3. A fiber optic telecommunication network that is used as communication link between the power grid and the SCADA infrastructures.

The reference scenario explicitly takes into account the set of essential services required for the correct functioning of the systems, the sequences of adverse events that could degrade the quality of such services, in terms of continuity, readiness, performances and time response. The model of the system of systems is therefore focused on the customer Quality of Services (QoSs) evaluation from the critical infrastructures operator point of view.

The electrical power produced in power generation stations is typically made available to the final customers through the transmission network and the distribution network.

The transmission network is similar to a meshed graph, in which every node is reachable through more than one path. The nodes of the graph represent the substations, while the arcs represent the transmission lines that connect the several substations. This topology make the network high reliable and available, avoiding that the loss of a single generator or a single line causes dangerous consequences.

The distribution network feeds consumers. The structure is mainly operated in a radial topology. The loads are connected to their substations in a star or in a ring with the aim of reducing service interruptions as a result of a major fault. The portion of electric MV distribution grid belonging to the current reference scenario is shown in Figure 8.

The main elements that constitute such infrastructure are the following:

- Two substations in which the electric power is transformed from 161 KV to 22 KV and splits to feed several customers. In our case, there are thirteen customers, of which six public, five commercial and two industrial customers;
- The electrical trunks which feed the final customers, connecting the substations to them.

The following interconnections in the MV electrical infrastructure, constituted by the electrical grid at 22 KV, are:

1. RTUs interface the portion of the MV power distribution grid with SCADA system;
2. Substations interconnect the portion of the MV distribution network to the portion of High Voltage (HV) transmission network.

The SCADA system consists of Motorola SCADAs that interfaces with Moscad TCP/IP Gateways and Field Interface Units (FIU) which manage the communication with RTUs, through elements such as Radio Frequency (RF) modem, called also MOSCAD, which convert wired signals to radio signals towards RTU.

The SCADA system is responsible for command and control operation on MV grid via graphical displays of switch operations and list of alarms.

The main SCADA functions are:

1. Acquisition and alarm of the Change of State of the MV switches;
2. Polling of the RTUs from the control center upon scheduled time, operator's request, and pre-defined event;
3. Graphical presentation of the current status of the MV switches;
4. Store of the history of Change of State of the MV switches.

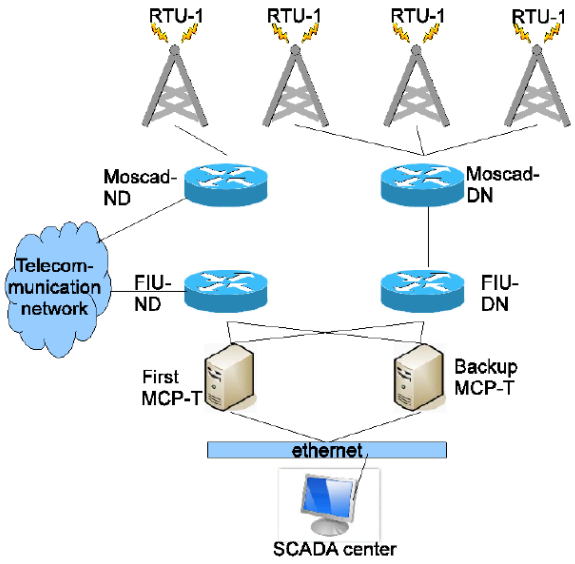

Figure 9: The SCADA network, for the case study

The other elements of the SCADA system reported in Figure 9 are described briefly.

The MCP-T is a gateway which converts the TCP/IP protocol in the Motorola proprietary protocol (MDLC) performed on the system. The MOSCAD FIU is a specific device dedicated to RTU interrogation and to the routing of data messages to/from the central. The FIU comprises RF modems. Each modem includes two VHF radio units, allowing field RTUs to reach SCADA centre on either channels. The Store & Forward Repeater is a special RF modem.

It is worthwhile to notice that SCADA is fully redundant. The topology of SCADA is reported in 9. The following interconnections have been discovered:

- With the MV power distribution grid by means of SCADA RTUs;
- With telecommunication network by means of the links between SCADA control centre and SCADA RTUs;
- The bus in SCADA control Centre is interconnected with telecommunication network;
- SCADA elements, such as RTUs and Control Centers are powered by the MV power distribution grid, adequately interfaced with a LV power grid and by means of an emergency power supply, typically constituted by UPS.

Usually, a telecommunication network is made of a core, a metro access and a customer access network.

The topology of telecommunication transmission network is reported in Figure 10. The network includes elements of the backbone, which are interconnected by Wavelength Division Multiplexing (WDM)

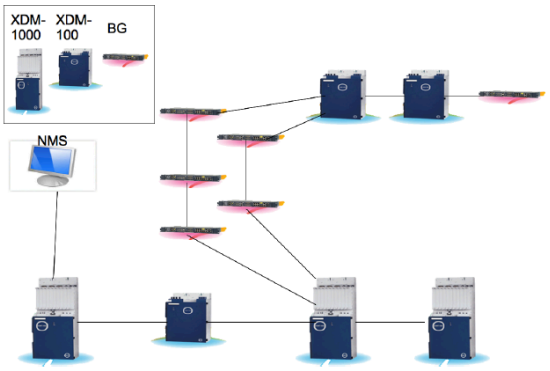

Figure 10: The telecommunication network, used in the case study

technology, elements of the metro access network, with SDH/STM-16 technology, and elements of customer access network with SDH/STM-4 technology.

The core network is based on ECI Telecom's XDM-1000s. These equipments are massive traffic concentrators which are installed in the heavy loaded metro-core junction. They support a wide range of data services. The metro access network is based on the ECI's XDM-100s. This network is characterized by the increasing demand by residential and business customers for higher bandwidth to support voice, data and video services.

The customer access network is based on ECI's BG equipments which are linked with other network by SDH technology. They deliver a mix of Ethernet, SDH and PDH services.

The Network Management System (NMS) enables efficient management of the communication transmission network. The NMS provides monitoring and supervision of the three levels of the communication network, by means of:

- Monitoring the fiber optical;
- Monitoring and managing transmission equipment network;
- Monitoring and managing the access network.

The following interconnections have been discovered:

- Some equipment of the customer access network are located into power grid substations, for example the substations (geographic interdependency);
- Some elements of the telecommunication network are powered by portion of the electrical infrastructure, constituted by the electrical grid at 22 KV, shown in 8, adequately with a Low Voltage (LV) power grid and by means of an emergency power supply, typically constituted by Uninterruptable Power Supply (UPS).

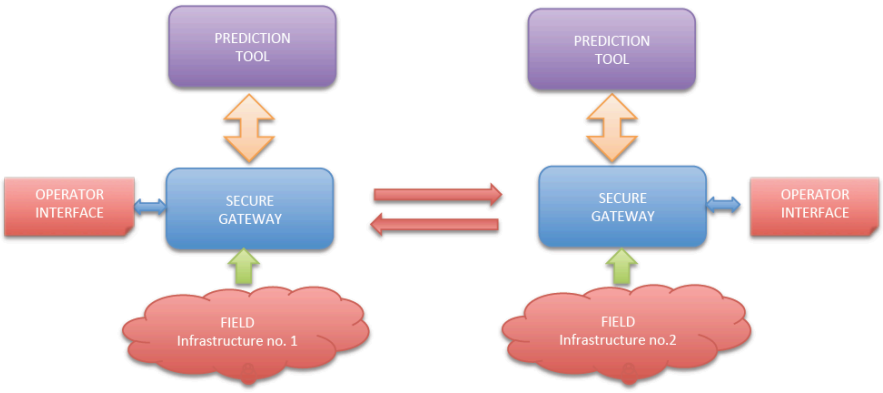

Figure 11: The online prediction tool configuration

1.5 ONLINE PREDICTION TOOL

The online prediction tool is a flexible and decentralized software tool that allows to connect different interdependent infrastructures and to compose the domain specific information of each sector in order to obtain a global estimation of the actual and future behavior of the System of Systems, based on a set of partial observations; each distributed tool, attested in a given infrastructures' control room, is equipped with an MHR model of the overall system and the model can be used to perform a short and medium term prevision of the working condition of the infrastructure and its subsystems. The underlying idea of this approach is that the single infrastructure, considering only its sector specific information may provide incomplete previsions, that do not take into account the interaction with the others.

For instance a power grid analysis software, although being aware of the disruptions occurring across the network, is not able to determine the congestion of a telecommunication network used to operate and reconfigure the electric branches remotely; conversely the telecommunication management software may be aware of the routing and packet flow, but is not able to forecast the occurrence of blackouts that may influence the working capability of telecommunication nodes.

Such a composition of information may also help discover domino effects and cascading failures; for instance a network congestion may interfere with the ability of the power grid to reconfigure the loads, leading to blackouts and thus exacerbating the critical situation of the telecommunication network and so on, in an ascending climax.

Figure 11 depicts the general structure of the online tool, whose main components are:

1. *Field:* each tool is attested in a given infrastructure and is fed with sector specific real- time data coming from the specific field; for instance the tool attested in the power grid infrastruc-

ture is aware of the state of transformers, generators and electrical customers, or the telecommunication infrastructure knows the traffic congestion, the operativeness of the equipments and the routing tables. The focus of the system is on the exchange of information and the synchronization of prediction; therefore the procedure for the retrieval of real time inputs used to feed the model was intentionally neglected and, in the case study, each tool used the original sensors and management systems of the particular infrastructure.

2. *Secure Gateway:* in order to avoid disclosure of sensible informations and to protect the information exchange among the tools, a secure gateway has been implemented for each tool. The gateway filters the huge quantity of information retrieved from the field and is responsible of the secure communication with the other tools and with the prediction tool; to this end a suite of security protocols have been implemented and the gateway adopts a web-service architecture based on the WS02 Carbon framework (www.ws02.com) and on X.509 [6] security protocol for the communication between the tools. Finally an ip filtering and an IPSEC [27] protocol has been set up for the communication between the field and the gateway and between the gateway and the prediction tool (for more details refer to the MICIE Project Deliverables [1]).

3. *Prediction Tool:* the prediction tool is the core module of the system, and it is responsible of the computation of the expected evolution of the system, based on the field data and on the data received by the other tools. At this level the discording data coming from the different information sources are composed and, once a consensus is reached among the prediction tools, the data is fed to the actual MHR interdependency model, computing a prediction of the state of the whole system (e.g., the power grid computes also the expected evolution for the telecommunication infrastructure, based on the data available, in order to capture interdependency phenomena that could not be captured by the single sector specific system).

4. *Operator Interface:* the interface is a set of linked graphical panels that summarize the actual and near future evolution of the system. The GUI offers different kinds of representations; an high-level interface is provided, where only the general state of the infrastructure (and of the other infrastructures as it is estimated locally by the tool), is represented. The interface offers also a comprehensive view of the reductionist components of the infrastructures; as shown in Figure 12, the operator has information about the actual state of the component (e.g., the component is marked with a red cross if it is down) and an

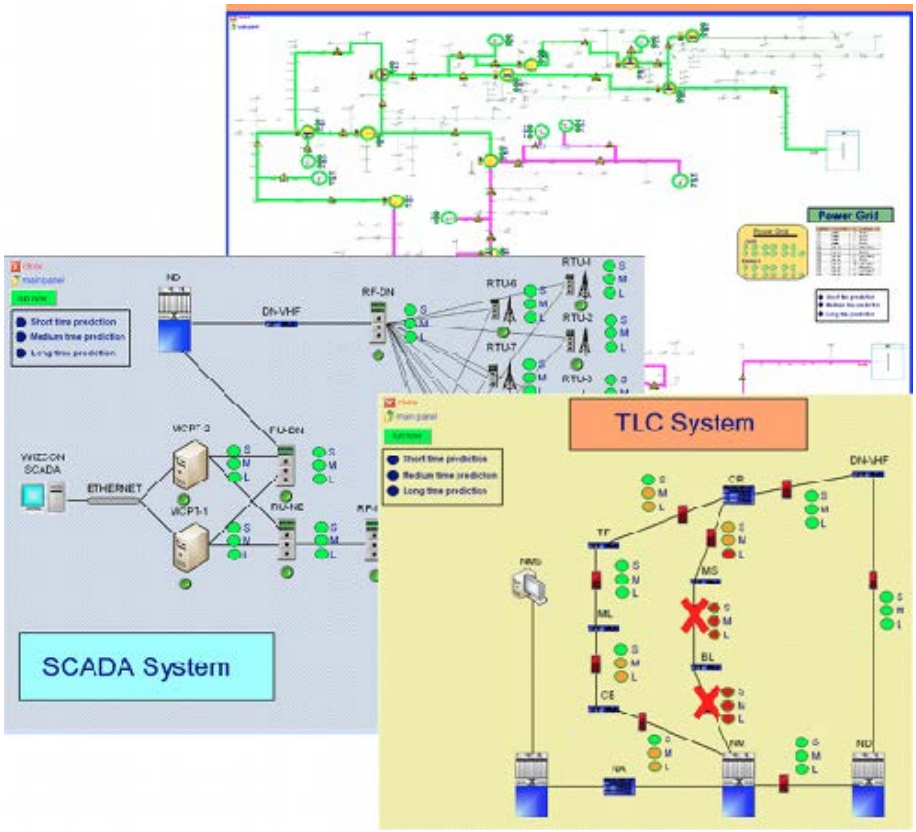

Figure 12: The operator panels

information about the expected state in the short (S), medium (M) and long (L) period, by means of three color indicators for each component, which act like traffic lights. In this way, besides noticing the actual failures, the operator is warned for possible future disruptions: for instance an orange medium time warning for an element in a secondary communication path in the telecommunication network, when the default route is not working may represent an expected congestion.

The proposed architecture therefore is aimed to compose partial observations by filtering the data coming from each infrastructure and exchanging information by means of a secure communication network; the distributed and peer to peer nature of the single tools allows great scalability in the case of multiple infrastructures.

Mathematically, this approach has been studied using the distributed consensus of arrays of systems with fuzzy variables, for further information [66, 68].

Figure 13 represents the case where the electrical infrastructure and the telecommunication infrastructures do not exchange data. In the example, for the sake of clarity and simplicity, only three entities are considered: a telecommunication node, the electrical reconfiguration service and an RTU.

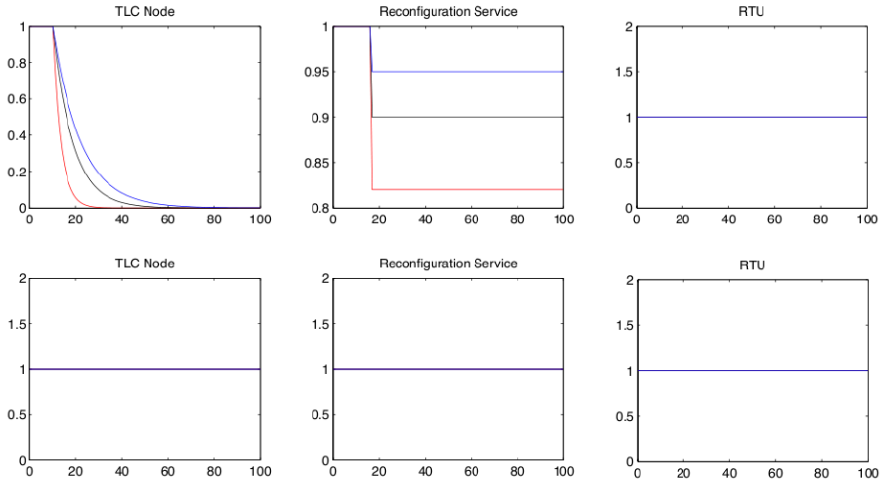

Figure 13: Example of isolated prevision

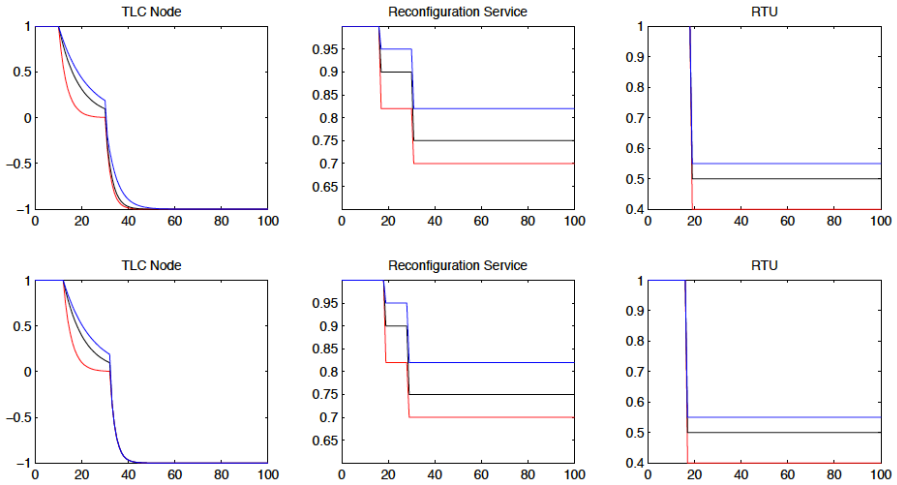

Figure 14: Example of composition of isolated previsions

The plots in the first row of Figure 13 represent the evolution of the state of the three entities seen by the telecommunication infrastructure, while the second row is the perception of the electrical infrastructure.

If at a given time instant a failure is detected on the telecommunication node by the telecommunication infrastructure, the working condition of the corresponding entity in the MHR model attested in the telecommunication infrastructure degrades; subsequently the model is able to predict a reduction in the working capability of the reconfiguration service, that is used by electrical technicians to operate remotely the power grid. Notice that, obviously, the electrical infrastructure does not receive information.

A completely different case is depicted in Figure 14, where the infrastructures communicate by means of the online framework. Besides agreeing on the severity of the failure on the telecommunica-

tion node and on the degradation of the Reconfiguration service, the proposed approach explicitly takes into account cascading failures and exacerbations; in fact the information received allows the electrical infrastructure to forecast a reduction in the working capability of the RTU. Such a new information, besides being passed back to the telecommunication infrastructure, generates further failures and exacerbates the existing failures, as shown by the Figure 14. Moreover it is possible to notice the presence of a slight delay due to the communication and consensus. Finally, note that the fuzzy formalism allows to take into account complex situations, where the best and worst cases are not symmetric; in the Figures the red, black and blue lines represent the evolution of the left endpoint, of the peak value and of the right endpoint of the triangle, respectively, and are associated to the best, mean and worst case. Notice that the distance between the curves is not regular, meaning different expectations for the best and worst cases. In this example the blue curve is always closer to the black one with respect to the red one, meaning that the best case is much more unlikely then the average and worst case.

1.6 CONCLUSIONS

This Chapter details the Mixed Holistic Reductionist Approach, based on CISIA software, in Sections 1.2 and 1.3. The main step is the validation of this methodology in a real on-line case study, described in Section 1.5.

A further enhancement has been the possibility of different structures: the centralised approach and the decentralised one. In the last case, the exchanged information among Prediction Tools is just the one related to services and highest node, i.e., holistic agents. In this way, the protection on real performance of infrastructures is achieved.

2

IMPACT ASSESSMENT OF CYBER THREATS

Recently issues about cyber-war have gained relevant attention, especially because of gravity of damages that could be caused by cyber attacks to strategic targets, mining security of citizens. Examples of targets might include national civil and military airports, command and control systems of civil and military transportation means electronic military systems for national defence, national infrastructures for water and electricity distribution, industries and also hospitals or fire-fighters informatics systems.

The risk of cyber attacks for the mentioned systems and infrastructures has grown because of the introduction of general-purpose and open (not proprietary) communication protocols, widely interconnecting systems and services.

With this regard, it is of great importance the problem of evaluating the impact that cyber attacks could generate and to select effective countermeasures to protect military and civil heterogeneous and interconnected systems.

The validity of MHR model has been already tested within the context of Critical Infrastructure Protection. In this Chapter, the effectiveness of the model is studied with regard to government infrastructure protection from cyber attacks and, with this regard, an explicative case study is presented.

This Chapter also proposes an innovative SCADA security test-bed that incorporates a Mixed Holistic Reductionist (MHR) methodology with SCADA network equipment. This technique performs an impact assessment keeping into account the existing interdependencies among Critical Infrastructures, controlled and supervised by SCADA systems. The main enhancement is the whole test-bed: a SCADA system with an impact assessment tool, able to visualize the forecasting outcome. The main effort has been on the finding the impact of different cyber attacks on the physical power grid: for example, how much the DoS can affect the behaviour of a breaker.

An application of the experimental framework to a sample scenario is presented in order to demonstrate the response of the system starting from detection of cyber attacks to impact evaluation of services delivered by each interdependent system.

2.1 CYBER THREATS

Improving decision-maker situational awareness within the cyber domain is not greatly different than enabling Situation Awareness in more traditional domains. The need of gaining Situation Awareness (SAW) (see also Chapter 3) arises when users deal with the problem of identify, understand and project situations, occurring in a specific domain, or even in complex and cross-domain contexts. Situations of interest depend on the context, as mentioned before, but also on the environment and on roles and goals of decision makers involved in the SAW process, anyway SAW methodologies can be defined in order to support any domain.

In this Chapter, Situation Awareness is considered in its broadest sense, as perception, comprehension and projection of the status of a system, following Endsley's definition [31]. For effective Cyber Situation Awareness [92], a crucial task is the identification of those activities individual decision makers are interested in and need to maintain awareness of over time. Once the activity of interests are identified and modelled, the observations necessary to identify the activities need to be defined. Another relevant aspect, besides to process analysis and model building, is the evaluation of the effectiveness of the SAW process implemented. The evaluation cannot rescind from the improvement of the cognitive process and decision making support. Anyway, measuring effectiveness for the proposed approach is still an open area of research.

Situation Awareness must be addressed to maintain users and operators not only informed of what is going in facility, but also conscious of the events. This process can be realized in two ways:

1. Model possible cyber attacks, define possible observations and in on-line mode try to recognize same attacks displaying events and already known information;

2. Model entire system, simulate in off-line mode some possible attacks, evaluate impacts or vulnerability on system and take into account the countermeasures to protect the on-line system from the most dangerous vulnerabilities and attacks.

In this Chapter, the framework proposed refers to the second approach mentioned. The methodology presented is called Mixed Holistic Reductionist approach (MHR) and it allows to model heterogeneous systems and to evaluate impacts of faults and attacks, through

the definition of different agents and their dependencies. The simulation model was originally thought to design critical infrastructures and their interdependencies, and to analyse their vulnerabilities in emergency situations as crisis after natural events (like earthquake or tsunami) or after some rare events that can lead to large outages for customers.

Within Critical Infrastructure Protection, cyber interdependencies are mainly due to the presence of SCADA systems, that make use of wide telecommunications networks to interconnect control rooms and the generic RTUs (Remote Transmission Units) in the field. In the past, SCADA systems employed proprietary, closed and specific protocols, as the Motorola MDLC. Recently, because of the development Internet, SCADA systems employ open telecommunications networks, such as the Internet itself, for the transportation of specific and relevant packages between the control room and RTUs.

All these changes in Industrial Control Systems increases the problem to protect these control system from cyber attacks and not only from the physical attacks. This issue is growing importance, also due to real experiences demonstrating how cyber attacks can affect also critical infrastructures.

The most popular attack is known as Stuxnet. Stuxnet [33] is a computer worm designed to affect industrial systems. Stuxnet infected Windows-based computers on industrial control systems. The worm is very complex, and its final goal was to reprogram Industrial Control Systems, hiding the changes to the operator. Stuxnet main features includes: zero-day exploits, Windows rootkit, first ever PLC (Programmable Logic Controller) rootkit, antivirus evasion techniques, complex process injection, hooking code, network infection routines, peer-to-peer updates, and command and control interface.

Other kinds of cyber attacks are those propagated from "inside": the infection starts in a workstation of the business/corporate network and then reaches the control system network and the control room. Another very common attack is carried out by compromise the Web-based interfaces to control room management systems exposed on Internet, by means of simply search engines like Google or ShodanHQ.

Cyber security government agencies, like Department of Homeland Security (DHS) and Australian Department of Defense Intelligence and Security, focus their attention on strategies for improving control system security and for mitigating cyber intrusions. These strategies provide guidelines for administrators on steps to take to ensure security confidence.

Infrastructures owners and operators are forced to act in accordance with national guidelines. Each facility should require a vulnerability assessment process to assess insecurities and make decisions about operating risks, and to make progress towards reducing risks

associated with control system operations. Vulnerability analysis provides a method of prioritizing the criticality of assets, threats and countermeasure strategies.

In recent years, researchers are focused on the power grid, and especially on the control system of power grids. Sridhan in [89] models a specific cyber attack related to data integrity attacks on a specific control area in SCADA power system. The approach extends cyber security attack concepts to control systems in an electric power system, especially on the Automation Generation Control (AGC) loop. Amin in [7] models stealth attacks on generic systems connected among them by telecommunication network, using game theory framework. This approach is independent from the specific facilities implemented in each node of the game theory.

Usually, the reference protocol is IEC 61850, which provides some generic features like the packet length and structure, for packet running on SCADA networks. In [75] authors described different kind of cyber attacks with possible countermeasures, specific for IEC 61850 transmission protocol. In [85], authors use the dynamic game theory to evaluate impact of several strategies for cyber network defences. A tool has been proposed in order to enhance understanding of cyber-network defence.

2.2 REFERENCE ARCHITECTURE

The network topology of the proposed SCADA security testbed is based on common SCADA network employing components such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electrical Devices (IEDs), Human Machine Interface (HMI) based on client/server architecture. All components are connected through an appropriate communication network. Innovative components consist of the Integrated Risk Predictor system (IRP) and a set of Intrusion Detection Systems (IDSs) that contribute to the task of impact evaluation of cyber risks on 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 University of "Roma Tre" and ENEA premises. Figure 15 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 (PCN-DB) stores information about equipment in the field. Data and information are visualized to operators through a specific HMI. Those information can be retrieved by means of a OPC (Open Platform Communication) server to other operators but also to the IRP (Integrated Risk Prediction Tool) which performs

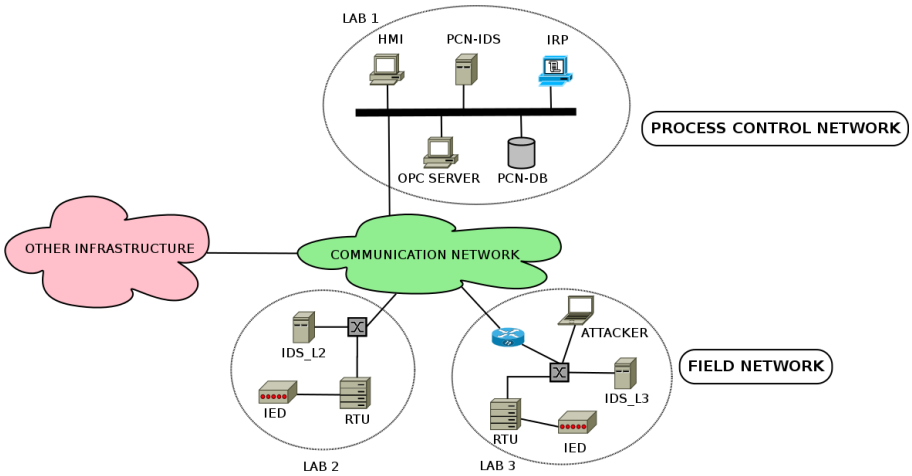

Figure 15: Reference architecture

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 (PCN-IDS) whose output is merged into the IRP.

- Field network: This network includes sensors, actuators (generally called IED) and RTUs and provides the acquisition of process field data and the execution of control actions. In addition, two IDSs (IDS-L2, IDS-L3), 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 host 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.

2.3 RISK PREDICTION TOOL ARCHITECTURE

Figure 16 presents the modular structure of the IRP. The IRP has six main units: the Mixed-Holistic-Reductionist (MHR), the failure acquisition (F-ACQ), the threats acquisition (T-ACQ), an OPC client, the Impact visualization (IMP-VIS) and the IRP database (IRP-DB).

OPC client. The main role of the OPC client is to query real-time data at a fixed time rate from the SCADA database (PCN-DB); such data will then be passed to the F-ACQ unit. Data coming from the SCADA system are related to equipment faults and failures.

Failure acquisition Unit (F-ACQ). 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.

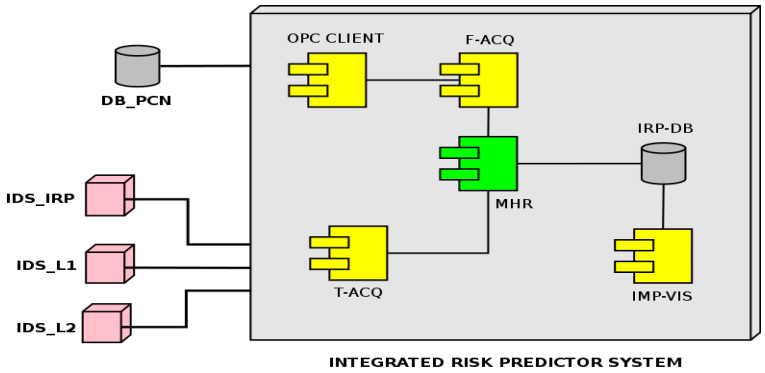

Figure 16: Integrated Risk Prediction Tool

The set of failures occurring on the components will then feed the MHR unit to perform impact assessment on the considered CIs.

Threats acquisition Unit (T-ACQ). 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. Communications between threats acquisition unit and IDSs are handled through web service technology: each IDS hosts a web service that accepts requests from web clients hosted in the Threats acquisition unit.

Mixed-Holistic-Reductionist model Unit (MHR). The main role of this unit is to perform impact of faults and attacks, through the execution of an agents-based model of heterogeneous systems including systems 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 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 affect it. In order to feed the MHR model, the Failure and Threats acquisition units provide real-time list of failures and malicious attacks to generate impact. A detailed analysis of MHR has been already given in Chapter 1.

IRP database (IRP-DB). The main role of this unit is to store results of MHR model executions in an appropriate database. Figure 17 depicts the ER model of the IRP database: two tables, named 'netelem' and 'fuzzytriangle' are dynamically updated at each IRP running step. The 'currvalue' view is defined as a join between the two previous tables and represents each agent of the IRP with its meaningful variables. At each variable is assigned a Triangular Fuzzy Number (TFN) in order to manage also uncertainty. This database also contains the 'historian' table that stores all previous data. This table is updated when the 'fuzzytriangle' table is updated.

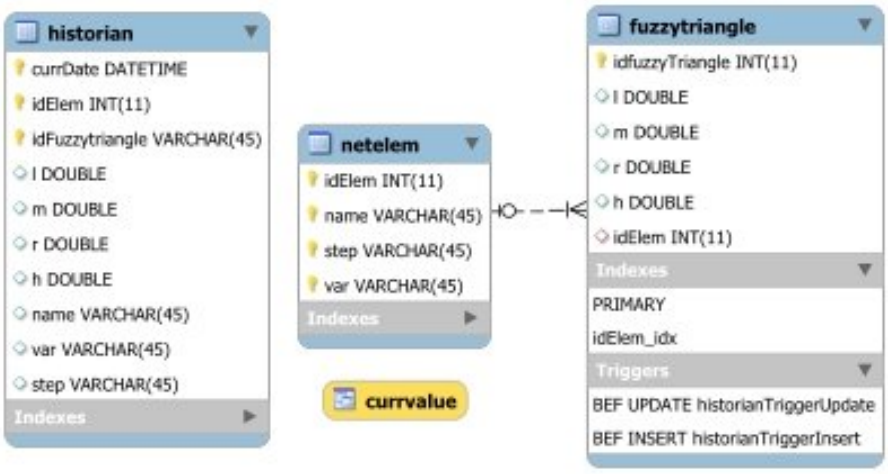

Figure 17: Integrated Risk Predictor database structure

Impact Visualization Unit (IMP-VIS). The main role of this unit is to provide the user with a Graphical User Interface (GUI) that shows the real-time impact of failures and attacks to the considered CIs.

2.4 MHR FOR CYBER ATTACK IMPACT EVALUATION

As already mentioned before, see Chapter 1, approaches to increase the security of Critical Infrastructures and systems can follow two different directions:

1. Models of cyber attacks are defined and then used to monitor the infrastructure by a set of distributed sensors: data fusion and inference techniques are employed to feed the model and allow the user to understand that a cyber attack is undergoing, so that he may try to block it.

2. Models of infrastructures are defined, than effects of cyber attacks are simulated, propagated and evaluated. Effective countermeasures can be applied as preventive measures.

As the definition of cyber attack models is not trivial, and could lead to too much simplified and inadequate models, the approach followed in this chapter is the second one. It requires a big initial effort in infrastructure modelling, but the derived model can then be used for different analysis.

Our idea is to test some cyber attacks, as worms, DoS, DDoS and Man In The Middle attack. All those attacks have outcome on the telecommunication network, without huge knowledge on the power grids. Other attacks as SQL injection, data injection or buffer overflow need the implementation for possible outcomes of specific modelling object in MHR modelling. Further enhancement are related to model a detailed SCADA system for power grids or Energy Management

System with several modules included databases, state estimation, optimal power flow, automatic generation control and so on.

However, MHR methodology can be applied in the cyber domain as described in the rest of the Chapter. All the agents inside the model follow a common general framework, following the basic idea of CISIA simulator [20]. Agents exist in order to produce, supply, transport or consume tangible or intangible resources: goods, policies, managements, operativeness, etc. Agents may be afflicted by faults or failures. The capability of each 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 affect it.

The internal representation of each single agent can be heterogeneous, however the coupling among the agents with several internal models is guaranteed by the respect of the common exposed interface.

In this context, it is necessary to differentiate among failures, according to their causes. Different kind of failures propagate their negative effects in different ways. A fault on a single equipment cause the absence of resources to the interconnected subsequent agents. If worms or viruses infect a telecommunication agent, as a workstation, consequences of the attack have effects on all telecommunication agents directly connected to the infected one.

Failures and their type can be contemplates also in other layers, than the telecommunication one. Cyber attack awareness and its cause identification leads allows to better evaluate the impact of faults on equipment and services, as well as to evaluate the QoS provided by infrastructures to customers.

As stated before, the focus of this paper is not on cause identification techniques, as discussed in [26], but on the evaluation of consequences of cyber attacks, in order to highlight system vulnerabilities and take effective countermeasures. Impact assessment is then estimated through simulations involving different equipment, supposed to be subjected to cyber threats.

2.5 EXAMPLE OF CYBER ATTACK IMPACT ASSESSMENT

In this section a simple case study is reported in order to support the effectiveness of the proposed approach within the cyber domain.

This reference scenario described hereafter will be adopted for simulation results. Let us consider the following three infrastructures, detailed in Chapter 1:

1. A power grid providing electricity to both civil and government customers (i.e. police offices, houses, etc.).

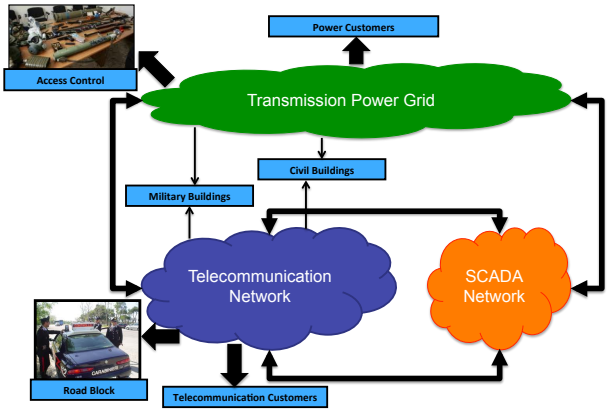

Figure 18: Interdependecies among critical infrastructures considered in the case study

2. A SCADA network, connecting power control rooms and the Remote Terminal Units (RTUs) of the mentioned power grid, connected to the tele-controlled breakers. The SCADA network is a particular telecommunication network, usually with a smaller bandwidth and specific protocols.

3. A telecommunication infrastructure connected to the SCADA network for packet forwarding to vary distant RTUs, and also for feeding, mobile or not, customers, as policemen around the city. This telecommunication network is connected to SCADA network through specific gateways.

A SCADA (Supervisory Control and Data Acquisition) system is a system specifically oriented to industrial system control and management. A RTU (Remote Terminal Unit) is an electronic device located in the field and connected with the SCADA by means of a telecommunication network, or in some case by means of serial socket.

Connections among infrastructures are shown in Figure 18. The power grid is controlled by the control center through the SCADA network. So, power grid equipment, as control centers or telecontrolled switches, are connected by means of specific gateways to telecommunication network. These gateways are included in SCADA network.

In the SCADA network, information is exchanged among control center and telecontrolled circuit switches. In case of failures on the power grid, the reconfiguration of network is necessary and this procedure is realized through command packets addressed to SCADA and to RTUs, in order to open and close the necessary switches. Moreover, all telecommunication equipment fed by the transmission power grid are fed by UPS (Uninterruptible Power Supply) system, not vulnerable to single power grid failures.

Breakers are components capable of interrupting the power flow in case of dangerous behaviour, i.e. short circuit. They are characterized by quick response and little closing and opening times, like millisec-

onds. Breakers are employed in protection and control strategies, but they can also be employed for operation and maintenance purposes.

Switches are devices adopted to physically separate power grid elements belonging to interconnected networks. Their response time to open/close orders are longer than the one of breakers. Consequently, they are regarded as elements to be operative after the intervention of breakers. The combined action of breakers and switches guarantees the complete physical and galvanic isolation of interconnected elements.

In the following, it is reported how the MHR approach can be applied to the scenario described before and depicted in Figure 18, where also possible end users of power grid and telecommunication network services are indicated. The three infrastructures have several interfaces, usually at reductionist layer. In fact some equipment are strictly related one to another, e.g. the RTUs of SCADA network with the power telecontrolled breakers. In this case in the MHR modelling, the interfaces are considered as two different agents, one for each infrastructure, by have a link able to transmit resources and failures. Always, the two agents, that are also interfaces between two facilities, have the same operativeness. Sometimes interfaces are the same objects, like for the telecommunication infrastructures and the SCADA network. In this case, at reductionistic layer, interface is modelled as only one agent that transforms resources and failures from one facility to another. These agents are connected to multiple holistic agents, due their interface nature.

The reference architecture we propose can provide a valid means to model the process of SCADA system vulnerability exploitations against cyber attacks. Our goal is to validate the IRP to analyse and assess the impact of cyber attacks on physical layer. Once an attack has been performed, the IDS produces a log file that is properly parsed and used by the IRP to evaluate the impact of such an attack.

In our research, we have implemented different attacks that compromise the security of SCADA system in the simulation environment and analysed the outcome of the IRP as a methodology for impact assessment. The objective is to assess the impact of a cyber attack on the reconfiguration service of a power grid (modelled with CISIA) controlled by the considered SCADA system.

A MITM (Man-In-The-Middle) attack has been performed in our test bed. 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 a MITM is to intercept a communication and modifying it to send fake data to the victim host. Our implementation of a MITM relies on ARP-poisoning (spoofing) attack. ARP-poisoning aims to modify the mapping between the MAC and IP addresses of the machines in the network by sending a fake ARP-reply to the victims.

Now the attacker can perform some actions: (i) disconnect A/B by simply avoiding to send the messages; (ii) loot the information contained in the messages; (iii) manipulate the packet content. In our testbed, A is the router that connects the lab to the HMI and B is the RTU. Our attack performs the ARP-poisoning attack by simply using a packet injector tool such as Ettercap to manipulate ARP tables. The attacker is now able to compromise the RTU e.g. by manipulating a message, or sending fake commands to the RTU.

The ability to perform a specific attack is strictly related to the rules needed by the IDS to discover the attack itself. In order to perform an ARP poisoning attack, the attacker may not be able to modify its IP address and in this case this action would be detectable by a simple IDS rule that keeps track of source and destination IP address. A more effective attack can succeed in changing the IP address of the attacker to be the same of the HMI or the RTU (IP spoofing) in order not to trigger the IDS rule. In our scenario, we used Snort [4] as IDS that allow us to detect ARP attacks, unicast ARP requests, and inconsistent Ethernet to IP mapping. In particular, we configured Snort to detect changes in the mapping between valid MAC and IP addresses: that allowed to detect ARP-poisoning attacks coming from the SCADA network.

Threats and Failures acquisition units depicted in 16 are needed in order to acquire data and information coming from IDSs and also from the HMI. The T-ACQ unit acquires data coming from the set of IDSs whereas the F-ACQ unit collects data coming from real equipment e.g. from the HMI. Connection between the T-ACQ and the IDSs is realized via web services technologies: each IDS represent the server, and the T-ACQ represent 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 OPC client/server architecture. T-ACQ and F-ACQ output are related to real equipment and services included into the MHR modelling architecture. These output are collected in a proper XML file whose structure is the same for both the units. A specific XML element specifies the attack type and; another element represents the severity of the attack by modelling it with a triangular fuzzy number.

The MHR modelling has been designed in order to evaluate impacts on interdependent CIs. This model has been updated aiming to consider not only mechanical faults and failures, but also cyber threats and their possible outcomes.

The case study depicted in Figure 15 is a general SCADA network, which is connected to a general-purpose telecommunication network for backup reasons. The IEDs are sensors and actuators for the considered CIs, in our case study they are remotely controlled switches and circuit breakers. The functionality and physical faults of the IEDs are obtained using the F-ACQ module from the SCADA database.

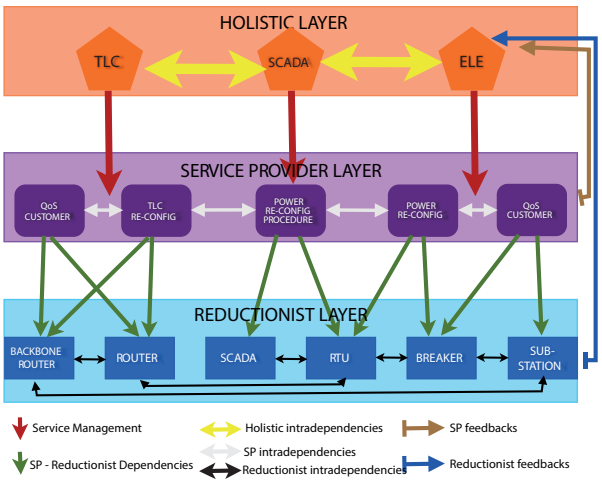

Figure 19: The case study modelling within MHR approach

The impact evaluation of cyber attacks (in our case a MITM - Man In The Middle attack) on the CIs allows to analyse how attacks can affect equipment and services. MITM attack can have several and several outcomes. The simple case is collecting information and acquiring knowledge on RTU and SCADA system, and their message exchange. In addition to read messages from HMI to RTUs, attacks can also modify the content of 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 vice versa). 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.

We considered the possibility that an attacker can drop the messages from the HMI to RTUs, especially those connected to actuators as circuit breakers and switches able to receive commands.

In the implemented model, service layer models the infrastructure capability to feed end users depicted in Figure 19, and it is able to reconfigure the infrastructure, triggering specific routines. In Figure 19, the most important agents and interconnections are depicted.

Following figures show the evolution of operative level of infrastructure components, when a MITM attack occurs on a RTU. Finally, we will assume that a second fault on the power grid distribution network occurs, and will analyse its effects on the already affected infrastructure.

Notes that the MHR approach manipulates fuzzy number, and especially Triangular Fuzzy Numbers (TFNs). These numbers are a way to express uncertainty. The triangular fuzzy number is defined by four (crisp) numbers: the left, the medium, the right value and the height. These values define an area, instead of a single number and are those plotted in the following figures.

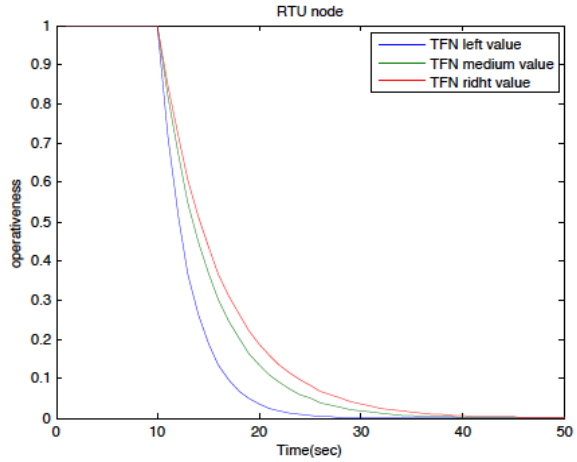

Figure 20: Operative level of a RTU agent

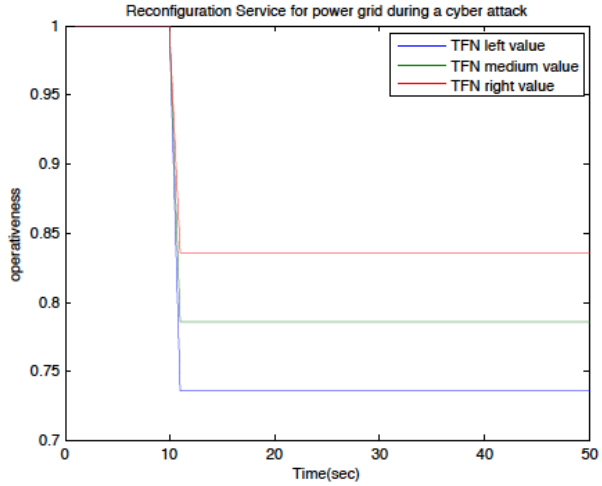

Figure 21: Operative level of reconfiguration service in the power grid infrastructure.

The behavioural trend of the RTU is depicted in Figure 20. We suppose that the attack start at 10 sec, and then the operative level of this node decreases with an exponential curve, reaching at 30 sec the completely inability to perform tasks.

Repercussion of the MITM cyber attack can be registered also in the power grid. If we consider only the packet dropping toward a RTU, no effects are shown on power grid, because the power grid in fully-operative conditions doesn't need telecommunication network.

Instead, in case of another fault, for example on the transmission power grid, the ability of the power SCADA to reconfigure the network is very reduces: the power grid reconfiguration requires packet transmission from the SCADA to the tele-controlled circuit breaker. This process aims to identify and isolate the fault area and then reconfigure the network by means of open/close commands. If packet

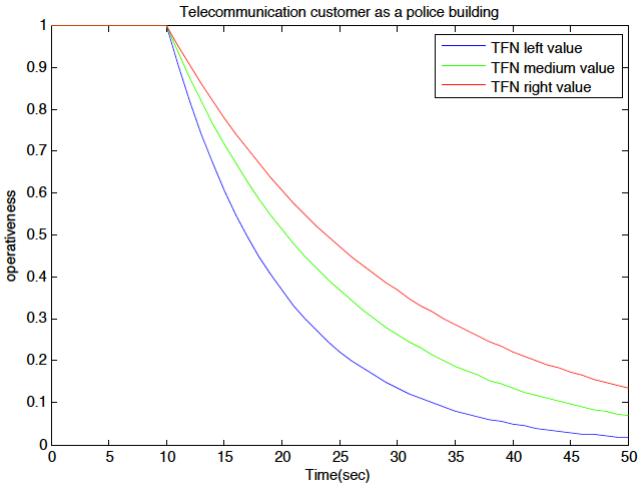

Figure 22: Operative level of a power grid customer.

transmission is not granted, the power grid reconfiguration service is strongly affected.

Figure 21 presents the operative level of the reconfiguration process for power grid. The reconfiguration process QoS decreases rapidly, because some configurations are not allowed, due to troubles in the communication channel.

Finally, the operative level of power grid service to an end user (i.e. the police building) is displayed in Figure 22. As it can be noticed, the telecommunication delay felt by users is slightly longer than the one in Figure 20. The trend is affected by possible reconfiguration of the power grids and also by different time scale of the infrastructures: telecommunication network is faster than power grids.

2.6 CONCLUSION

This Chapter details the enhancement of the MHR modelling with cyber treats inputs: the main enhancement is due to impact assessment on real equipment of cyber attacks. This evaluation is dependent by the real working and functionality of the infrastructures. The other drawback is the necessity of the MHR to model all the equipment and software modules that are affected by the selected attacks.

The possible outcomes of cyber attacks are a very important aspect in the research on Critical Infrastructure Protection, but we need a possible taxonomy of actual cyber threats in Industrial Control Systems, and their possible outcomes.

3

SITUATION AWARENESS: MODELS AND METHODOLOGIES

In the context of Homeland Security there is the urgent need to suitably aggregate raw data obtained from multiple and heterogeneous information sources in order to provide deeper insights on the high level situation as well as on the behaviors of the different agents or entities (e.g., enemy ships, cargo or pleasure boats), and their possible interactions.

This Chapter reviews some of the most diffused methodologies for the fusion of different low-level information sources in order to provide an increased awareness on the ongoing situation, describing a possible case study with pros and cons. The topic is particularly relevant in the context of homeland surveillance (e.g., land or marine patrolling), where a huge amount of information is typically available.

After a brief review of the basic notions related to Data Fusion and Situation Awareness, the most adopted strategies for the extraction of qualified high-level information from sensorial data will be illustrated and critically compared.

3.1 SITUATION AWARENESS

While attempting to perform any homeland surveillance strategy, an essential step is to define and implement methodologies for the assessment of the actual situation, as well as its near-future evolution.

Field surveillance activities 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 purpose of identifying them on the base of their behavioural characteristics, and to cataloguing them according to their potential intent (e.g., pirate vessel). In other terms, the surveillance activities

encompass the following 3 questions: WHO,WHAT and WHY; WHO is inside the patrolled area, WHAT it is doing (e.g., the actual situation) and WHY is there (which is its intent).

This is however a non-trivial task, since any single sensor by itself usually does not allow to exhaustively answer to the above questions, especially in the presence of smart enemies, since it may provide ambiguous information. For example, the presence of an unknown object detected by a radar in a patrolled maritime area may indicate a fishing boat or a refugees' ship, rather than an attacker. Thereafter, there is the need to carefully inspect the behavior of the entities that act in the considered scenario according to multiple perspectives in order to acquire awareness on their intent and on the associated threats. Moreover, this has to be done for a reasonable amount of time, in order to assess complex behaviors. Note that, also given the challenging complexity of the task, no exact guideline can be given in this sense.

Hence, it is fundamental to provide adequate raw data aggregation methodologies, in order to obtain high-level pattern or behavior detection and prediction: this is the objective of *Situation Awareness* (SAW) techniques.

In 1995 Endsley [31] defined Situation Awareness as "knowing what's going on" or, more formally, 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".

Situation Awareness is strongly related to the temporal dimension; the main idea is, therefore, to use knowledge acquired in the past to identify, analyse and understand the actual situation and to forecast its evolution, with the aim to evaluate the risk.

Therefore, the field of Situation Awareness is directly connected to the Data Fusion problem, where multiple information sources have to be combined, in order to gain insights on the situation [55]. Such problems arise in many contexts, e.g., in the military field, in the field of environment surveillance and monitoring, in robotics and in medical diagnosis.

In this Chapter, some of the most diffused methodologies for the fusion of multiple and heterogeneous information sources will be briefly reviewed and critically compared, having in mind the final objective to increase the awareness on the ongoing situation in a dynamic scenario characterized by non-trivial complexity.

3.2 SITUATION AWARENESS MODELS

The most adopted data fusion schema is the *Joint Directors of Laboratories* (JDL) model [32].

The JDL is a 5-layered hierarchical model, where each level is aimed to provide a more abstract, high-level and descriptive representation

of the scenario. Indeed, while proceeding from the lower to the higher levels, the degree of abstraction is increased, and the amount of information is reduced due to the aggregations performed at each level. Note that, at each level, the model theoretically provides a prediction of the expected evolution for the scenario.

Let us now describe these levels, which are defined as follows:

LEVEL 0: SUB-OBJECT DATA ASSESSMENT At this layer the single signals are taken into account. The amount of data gathered at this level can be quite relevant, hence having a very low degree of abstraction (e.g., spatial occupancy of a grid, audio/video streams, etc.). Moreover, a first identification of the objects and entities involved in the scenario, along with a first low level prevision of their behavior (e.g., trajectory interpolation), is provided.

LEVEL 1: OBJECT ASSESSMENT At this layer, based on the sensorial information of the level below, the objects are estimated and their behavior is predicted. In this way it is possible to perform the tracking of the entities, eventually involving multiple sensorial information.

LEVEL 2: SITUATION ASSESSMENT At this layer the relations existing among the entities are evaluated and predicted. This is the level where complex behaviors are identified (e.g., surrounding, side attack, refueling, etc.), taking also into account the physical context (e.g., constraints in the movements due to obstacles).

LEVEL 3: IMPACT ASSESSMENT Estimation and prediction of the effect and impact of the identified situation/actions on the actors and entities involved (e.g., expected damages and losses given the enemy's behavior). At this level planned actions between the plans of multiple players (e.g., assessing susceptibilities and vulnerabilities to estimated/predicted threat actions given one's own planned actions) are also evaluated.

LEVEL 4: PROCESS REFINEMENT This level is aimed to adaptively tune the information and the insights obtained by the lower levels, based on the data acquired and on the extrapolations made from such data, in order to refine the understanding and provide a support to decisions, highlighting the impact of these decisions.

Hence, the actual assessment of the ongoing situation is mainly performed at level 2, while the prevision is mainly done at level 3. The interested reader is referred to [55] and [32] for a thorough discussion.

Another established Situation Awareness model is the so called *Boyd Control Loop* [12], often referred to as OODA loop, since it is composed of the four phases: Observe, Orient, Decide and Act.

The OODA model can be partially mapped into a JDL model: the Observe phase can be compared to the JDL level 0, while the Orient phase encompass the JDL levels 1, 2 and 3; the Decide phase is mapped into JDL level 4, but it also includes logistics and planning; the Act phase has no direct analogue in the JDL model, and it can be seen as the actual decision made based on the JDL framework. Consequently, note that the actual SAW activities are performed within the Orient phase.

The main attractiveness of the OODA model is that it closes a loop between sensing and acting, thus providing a more resilient methodology with respect to changes in the environment or in the enemy strategy. However such an approach lacks in the ability to assess the impact of the Decide and Act phases on the other phases of the loop, that is instead performed by JDL level 4.

A possible evolution is to close a loop at each level of the OODA model, and to consider the interaction among these loops [84].

Notice that both JDL and OODA models are not sharply defined and do not imply a unique implementation; in fact some activities are present in multiple levels or steps. Hence, JDL and OODA should not be considered as operative procedures, but have to be treated as logical schemas that may help to better organize the information and to adequately define the steps for the extrapolation of high-level and abstract information, based on raw low-level data.

In next Sections some of the most established methodologies to perform Situation Awareness will be described. As stated previously, a system increases users' SAW if it is capable to understand what is going on in the observed scenario, and if it is capable to foresee its evolutions.

The aforementioned capabilities correspond to JDL levels 2 and 3, and to the Orient phase of the OODA model, regarding the assessment of situations and the evaluation of related threats, through situation projection.

3.3 METHODOLOGIES

Hence, the methodologies performing SAW must be able to reason about the ongoing situation starting from observations acquired from heterogeneous sensors. With this regard, in next sections the following techniques will be presented:

BAYESIAN BELIEF NETWORK: this technique is based on a probabilistic approach. It uses Bayesian Nets to model hierarchical, cause-effect relationships among relevant aspects of the situation of interest. The net is characterized by probabilistic weights and the belief related to each node is computed taking into account weights and the observations gathered from the field. Observations can be heterogeneous and can be posted at each level

of the net, updating the belief of the states of the net. Evaluating the beliefs of all nodes of the net, the user is able to understand the on-going situation. An extension of such a methodology are the Dynamic Bayesian Net, that allows to compute the beliefs of the nodes of the net, in future time stamps, i.e., projecting the assessed situation and therefore they allow also to evaluate threats.

MARKOV MODELS: also this technique is based on a probabilistic approach. It allows to model time-dependent situations, through a graph whose edges are weighted by probabilities. Once observations are gathered, it is possible to estimate the most probable path on the graph, that is the most probable on-going situation and also it is possible to estimate which is the state of the observed situation. Moreover, according to the model, it is possible to say which is the most probable state of the graph, i.e., to project situations and, consequently to evaluate related threat.

NEURAL NETWORKS: this approach is largely used to reason about complex situations, whose model, eventually non-linear, are defined by learning algorithms. Within such a framework, the situation of interest is represented as a black-box, which can be fed with heterogeneous observations. Even in this case, the evaluation of values of output variables, representing the situation of interest, allows user to be aware of a situation. This technique does not suit projection capability.

EVIDENCE THEORY: this technique is based on the theory of possibility. It allows to model knowledge about time-independent situations, thanks to bipartite graphs, correlating causes (situations of interest) to effects (observations). Evidence theory handles uncertain, heterogeneous and eventually incomplete observations and identifies the most plausible subset of situations occurring in the observed scenario. This methodology allows also to aggregate low-level data in order to give them a semantic meaning. This meaning can be used as input to other knowledge models, eventually more complex (e.g., Markov Models), allowing to reason about time-dependent situations and therefore to perform threat assessment.

For what stated before, techniques presented in this Chapter can be employed to implement Situation Assessment, and, in some cases, also Threat Assessment, increasing the awareness of the user.

3.4 CASE STUDY

To highlight the differences and to critically compare the methodologies analysed so far, in the following a case study will be considered. The case study is a modification of that provided in [105].

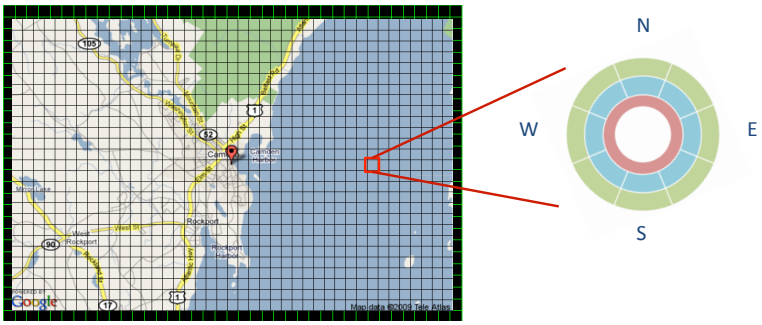

Figure 23: Example of maritime surveillance scenario

Consider a maritime surveillance problem, where a coastal and maritime area has to be patrolled, and the behavior of the ships in the scenario has to be assessed based on sensorial information. Specifically, suppose to partition the area into a tessellation of small uniform zones of the desired size, and suppose that the position of a ship is identified by the zone where it is detected (see Figure 23). Suppose further that it is possible to obtain information about the velocity and direction of the ship. Let us assume that a ship may have one of the 8 directions depicted in Figure 23, while 3 different velocities are considered for each direction, i.e., fast (green), slow (blue) and zero (red). Finally, for the sake of simplicity, let us suppose that only one ship is present in the marine area of interest, and that the possible behaviors for the ship are: attacker, pleasure boat or refugees' ship. In the following some hints on how to set up a situation assessment framework based on each of the methodologies described in this Chapter is provided. For deeper analysis on the different methodologies please refers to [25].

BAYESIAN NETWORKS Due to the dynamic context of the problem at hand, a static BN seems not adequate to assess the behavior of the ship. Hence, a good choice is to rely on a DBN, as shown by the example in Figure 24. Specifically, n Bayesian networks are considered for n time steps. Let us assume that each BN has a root node (ship behavior) and 3 leaf nodes (position, velocity and direction). In order to take into account the temporal dimension, the n networks are interconnected, by linking the input node of each BN for time $t, t-1, \ldots, t-n$ to the leaf nodes of the BN. Note that the complexity of this method can be overwhelming, since the number of states is indeed huge. Note further that such an approach allows both to

assess the belief of a sequence of position/velocities/states given the actual behavior in a forward prospective and to determine the behavior based on the previous n time steps using the backward mode. However, it is not possible to handle loops in this context. In Figure 24 the behavior of the ship is assessed based on n linked Bayesian network, each focusing on a particular time step (only the first and the last BN are reported in the Figure). Specifically each BN considers the relation between position,velocity and direction of the ship and its behavior at a given time step.

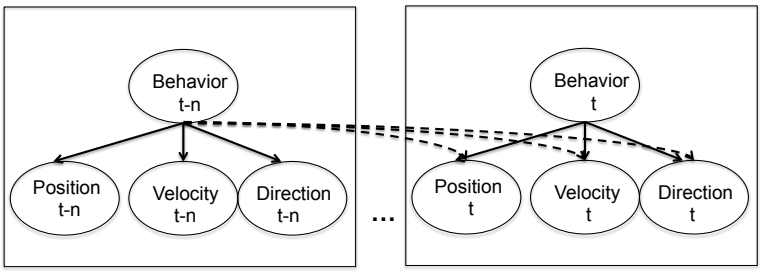

Figure 24: Example of dynamic Bayesian network for maritime surveillance

ARTIFICIAL NEURAL NETWORKS Figure 25 represents an example of ANN aimed to identify the behavior of the ship: the values of position,velocity and direction for n steps are used as input in order to identify the ships' behavior. Since the setup of ANNs requires a huge availability of input/output couples, differently from the above case, it seems natural to consider an input layer containing the values of position, velocity and direction of the past n steps. In the example, the network is composed of 2 intermediate layers of neurons, and has an output layer with a node for each behavior. Although being similar to the DBN example above, there are some significant differences in this approach. First of all, besides the direction of the links, the input/output values need not to be probabilistic, hence the ANN framework is more general. Moreover it is possible to consider many complex subsequent layers, without needing to assess the CPT of each node; in fact the learning methodology for ANN assesses a reduced set of parameters with respect to BNs. Note further that the graph topology varies during the learning phase, allowing finer representations with respect to the a priori knowledge of the interaction among the layers. Finally, the value associated to the input nodes need not to be a discrete value, hence it is possible to consider more realistic data (e.g. the actual GPS position, the velocity in mph, the direction angle) without increasing the complexity of the system. Analogously to BNs, however, a learning procedure has to be set-up, hence there is the need to consider a huge set of trajectories, along with the corresponding expected behavior. Nevertheless, the complexity, in both

BNs and ANNs, significantly grows with the time window considered for the input data (e.g., number of time steps), and the paradox is that a small n may not be descriptive of the behavior, while a big n may not be feasible.

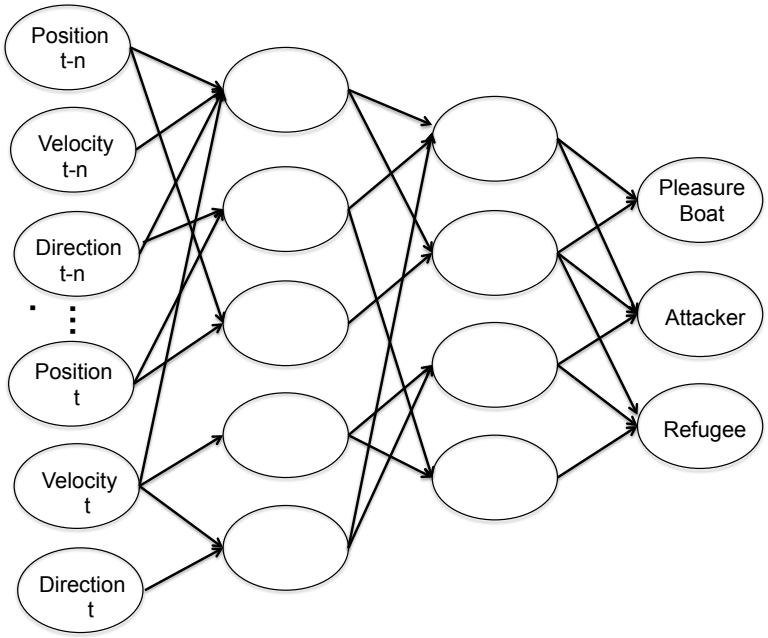

Figure 25: Example of ANN for maritime surveillance.

MARKOV MODELS Figure 26 shows an example of MM and an example of HMM for the scenario at hand. The leftmost figure represents an MM where the states are the positions in the grid. Specifically, in the figure only the states directly reachable from the red node are represented: the blue ones are the 8 cells contiguous to the red node (i.e., reached in one step with “slow" velocity) and the green ones represent a jump of two cells (i.e., “fast" velocity). The rightmost figure represents an HMM where the position information is hidden and only velocity/direction information is available. Specifically, in the proposed example, a node represents a position on the grid, and the Figure represents the neighbourhood of a given node. Within the MM example, the node in red is connected to 8 nodes (in blue) representing the 8 cells in the grid contiguous to it (along to the 8 directions considered) and associated to the velocity “slow". Moreover, 8 additional nodes are considered (in green) that represent a jump of 2 cells along the 8 considered directions. The set of arcs is completed by a self-pointing link, representing the permanence in the same cell. As shown by the example, the number of states coincides with the size of the grid, but the number of links is non-trivial in this setting.

Consider the case where the position can not exactly be assessed, but the information on direction and velocity can be obtained (e.g.,

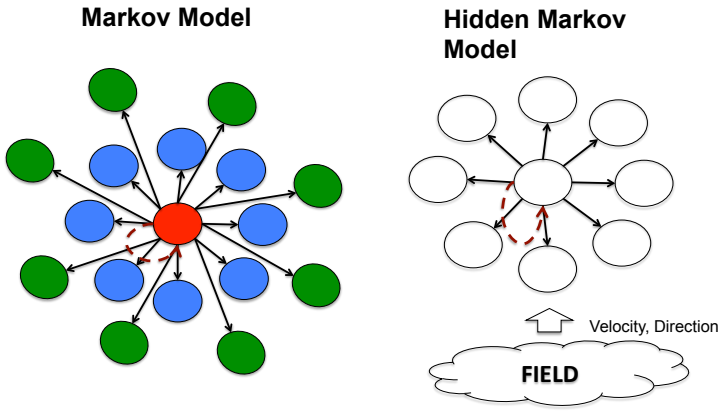

Figure 26: Examples of MM and HMM for maritime surveillance

by interpolating a noisy trajectory). In this case the HMM depicted in Figure 26 can be considered, where the vector of states (e.g., positions) has to be assessed based on the information on velocities/directions, by means of the Viterbi algorithm. In this case the number of links can be reduced.

Note that, in both cases, a non-trivial issue is how to define the transition probabilities: if in the HMM case it seems natural to set the probability of each of the 9 outgoing edges for each node as $1/9$, it is less clear how to choose the probabilities in the MM example; for instance the probability to make a jump of 2 cells has to be associated with a smaller probability with respect to moving of 1 cell or remaining in the same cell. Note that the HMM setting may also take into account other typologies of observation; for instance it may be possible to consider a witness that has a vague idea of the position, or an audio recording that can be used to assess the size of the boat and hence the possible velocity.

Let us now provide an alternative to HMM for the assessment of high-level states by means of the Evidence theory approach.

EVIDENCE THEORY Figure 27 reports a simple application of the Evidence Theory framework. In the figure 2 out of m information sources are reported; specifically, the figure shows that the same set of information $\{\omega_1, \omega_5\}$ can be mapped differently onto the set of directions, although partly overlapping. Suppose that m different information sources have access to low level or raw information and have to assess the direction of the ship. Each of the information sources has a subjective idea on how the informations have to be mapped into the 8 directions. In the picture only 2 associations are depicted; note that the images of the combination $\{\omega_1, \omega_5\}$ partly overlap, thus leading to a higher probability associated to the direction North (N). Note further that a huge set of associations might be defined and, in particular when multiple information sources are considered, the

complexity may rapidly become unmanageable, since the complexity is exponential in the cardinality of the associations.

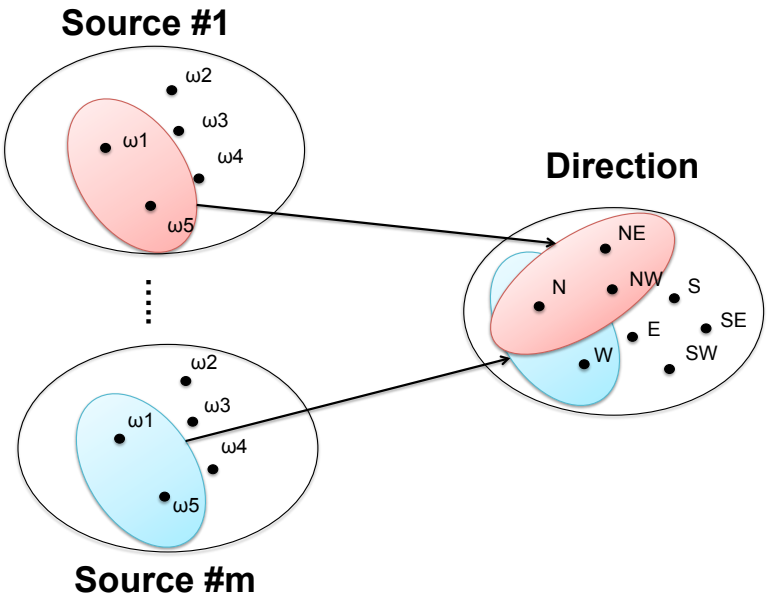

Figure 27: Examples of assessment of the direction of a ship based on Evidence Theory

Such an approach, however, can be considered as a prerequisite for all those cases where an high level information (e.g., the direction), although required by a situation assessment algorithm, is not directly available.

3.5 CONCLUSIONS

This Chapter aims to briefly summarized the most used methodologies in Data Fusion for Situation Awareness, presented at a very general level without information related to the underlying techniques. A simple case study is described in order to explain differences among these techniques.

4

NETWORKED EVIDENCE THEORY

This Chapter shows the application of a distributed approach of information fusion and sharing, based on the Evidence Theory and the Transferable Belief Model (TBM), to the field of Critical Infrastructure Protection. Evidence Theory can be successfully used to aggregate information generated from different sources, in order to better assess the ongoing situation of the overall system and then help the infrastructures' operators in a decision making process.

In the field of Critical Infrastructures, as a consequence of the existence of several stakeholders, and due to existing interconnections among facilities, researchers are forced to develop distributed approaches in both modeling and control, with a minimum exchange of information, and eventually with a high level of security.

Evidence Theory, not only allows the modeling of uncertainty in information fusion, but can be effectively used in a decentralized way to guarantee the convergence to the same results obtained in the case of a centralized approach. We propose a case study consisting in the aggregation of sensor data to identify the causes of a fault in one infrastructure; fault that is supposed to affect other infrastructures too, generating measurable effects on them. The same algorithm could be applied to different degrees of abstraction allowing, for example, a risk analysis in a decentralized fashion.

4.1 INTRODUCTION

Evidence Theory is a methodology that is often considered when dealing with Data Fusion problems. Data Fusion [19] means combining information generated from heterogeneous sources or sensors to devise an estimate of the ongoing events. Modern Data Fusion is an automated process that enables the determination of a situation with a high level of abstraction, assessing objects and also estimating

possible risks, finding anomalies or failures, and helping people to take decisions.

Evidence Theory comes from Shafer's work [83] who expanded the Dempster's theory [22]. Evidence Theory is sometimes compared to Bayesian Networks. This latter approach allows the recognition of the input values as likelihood from some pre-determined patterns. The difference between the two methods is in dealing with uncertainty [62]. Dempster-Shafer theory (DS) considers explicitly the uncertainty thereby it allows to understand whether the various sources of information are inconsistent or if there is an error or uncertainty in the modeling process. The validity of the two approaches depends on the type of applications and the kind of knowledge that has to be represented and fused [63].

The Dempster-Shafer (DS) framework [83, 22] generated by multivalued mapping, leads to the definition of lower and upper probabilities as belief and plausibility functions. Different rules for combining the available information can be considered within the DS framework. The methodology used in this article is the one proposed by Smets in [87], which extends the DS framework by assuming that the correct answer might not be among the considered ones (open world assumption). Furthermore, the approach proposed by Smets allows the computation of the amount of contradictory information in the value of the empty set.

The major limitation to the application of the Evidence Theory in a real context is the number of hypothesis required for modeling the application of interest. This can be explained by the fact that from a computational perspective, the power-set of those hypotheses has to be computed and its complexity grows exponentially with the number of hypothesis. In a large number of practical cases the Evidence Theory has been successfully applied and, to overcome such difficulties, some authors [97, 49] have also proposed approximated approaches.

In this Chapter Evidence Theory has been applied to the real case of information fusion and sharing between Critical Infrastructures (CIs). Those systems are necessary to the welfare of civil society and are interconnected with each other through various kinds of physical and logical links. Modeling those interdependencies is sometimes a complex task but it turns out to be necessary, for example, to correctly analyse cascading phenomena. Interdependencies, from the point of view of Data Fusion, can be also seen as a source of possible information. Indeed, a global situation assessment can be sometimes inferred using data coming from different control rooms. In particular, this works focuses on the possibility of reconstructing the cause of a critical event from measures that can be performed by sensors related to different CIs. These events have two main characteristics: a low probability but a high impact. Impact that is not limited only to the

infrastructure where the fault is detected or generated, but can also propagate to other infrastructures interconnected with the first one. This means that a "signature" of the event can be found in the interconnected system almost everywhere, and sometimes, also in independent agencies like meteorological services or police departments. There is, hence, the need of fusing together all available data to build a common vision of the current situation, to take the correct decision and choose the best action plan. In this view, it should be noticed that Critical Infrastructures are inherently distributed [21] and thus, also the fusion mechanism should be distributed, perhaps providing an encryption layer for the the transmission of information of shared information as well.

It is worth noticing that Data Fusion outputs, for example the possible causes of a failure, can result of great help in impact assessment. In fact, limiting impact assessment to measured events can lead to heavy underestimation, or wrong estimation, of impacts in many cases. For instance, an isolated failure of an appliance can be propagated in a very different way if it is due to a fire blast detected by a sensor or a computer virus signaled by an Intrusion Detection System. In the first case it will be propagated in an interdependency model according to a spatial proximity pattern, while a computer virus would spread among similar telecommunication nodes, even if they are far.

An impact assessment tool must be able to manage the situations and their confidence levels. Note also that Data Fusion outputs are uncertain, so the impact assessment modeling approach must consider unreliable input data. A possible approach is fuzzy logic to manage lack of certainty. Among the others, CISIA (Critical Infrastructure Simulation by Interdependent Agents), [72, 21] is an agent-based simulator, using Triangular Fuzzy Numbers, to represent involved quantities.

This Chapter describes how the distributed Data Fusion framework proposed in [40] based on the Theory of Evidence can be successfully applied to the field of Critical Infrastructure for situation assessment.

4.2 EVIDENCE THEORY

Evidence Theory [83, 22, 87] is a mathematical formalism for handling uncertainty starting from the knowledge inside the evidences. The idea is to evaluate the support and the plausibility functions for each set of hypothesis, to reduce uncertainty and help finding the set which contains the true answer to a question.

Define $\Omega = \{\omega_1, \cdots, \omega_n\}$ as the set of hypotheses that must be considered as the set of possible value of the variable ω. This set is called *frame of discernment*. For example, the possible causes of failures of a critical infrastructure could be a sabotage, the failure of an appliance, a fault due to the weather, or, for instance, a cyber attack. In

the Theory of Evidence the hypotheses are assumed to be mutually exclusive.

Starting from the frame of discernment, it is possible to define the *power set* as $\Gamma(\Omega) = \{\gamma_1, \cdots, \gamma_{2^{|\Omega|}}\}$, that has cardinality $|\Gamma(\Omega)| = 2^{|\Omega|}$. This set contains all possible subsets of Ω, including the empty set $\gamma_1 = \emptyset$ and the universal set $\gamma_{2^{|\Omega|}} = \Omega$.

The Trasferable Belief Model (TBM) [87] is based on the definition of a *basic belief mass* function: $m = \Gamma(\Omega) \rightarrow [0; 1.0]$. This function is a map that assigns to each element of the power set a value between 0 and 1. This function, also called *basic belief assignment* (BBA), shall respect the following constraint:

$$\sum_{\gamma_a \subseteq \Gamma(\Omega)} m(\gamma_a) = 1 \quad \text{with} \quad m(\emptyset) = 0 \tag{2}$$

Each element γ_a having $m(\gamma_a) \neq 0$ is named *focal set*.

In this framework, the interest is focused on quantifying the confidence of propositions of the form: "The true value of ω_i is in γ_a," with $\gamma_a \in \Gamma(\Omega)$. For $\gamma_a \in \Gamma(\Omega)$, $m(\gamma_a)$ is the part of confidence that support exactly γ_a. This means that the true value is in the set γ_a but, due to lack of further information, we are not able to better support any strictly subset of γ_a. This is not a probability function, and it does not respect the property of additivity: $m(\gamma_a \cup \gamma_b) \neq m(\gamma_a) + m(\gamma_b)$.

Each BBA is an atomic element within the TBM. In fact, each sensor, agent or node must be able to assign the BBA values by some subjective assumptions, or through appropriate algorithms that automatically determine the assignment.

In the case of different independent informations sources, a rule to aggregate the information must be provided.

There are many rules of combination in the literature. Among the others, the most widely used are the Dempster's rule and the Smets' one.

The *Dempster's rule of combination* is a purely conjunctive operation and was the first to be formalized [22]. This rule strongly emphasises the agreement between multiple sources and ignores all the conflicting evidence through a normalisation factor, as shown in Equation 3. This has the effect to attribute null mass to the empty set. So the rule is formalized as:

$$\text{Dempster}\{m_i, m_j\}(\emptyset) = 0$$

$$\text{Dempster}\{m_i, m_j\}(\gamma_a) = \frac{\sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c)}{1 - \sum_{\gamma_b \cap \gamma_c = \emptyset} m_i(\gamma_b) m_j(\gamma_c)} \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{3}$$

Differently, the *Smets' rule of combination* [87] allows to express explicitly the contradiction in the TBM, by letting $m(\emptyset) \neq 0$. This combination rule, compared to the Dempster's one, simply avoids the normalisation while preserving the commutativity and associativity properties. The formalization is as follows:

$$\text{Smets}\{m_i, m_j\}(\gamma_a) = m_i(\gamma_a) \otimes m_j(\gamma_a) \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{4}$$

where

$$m_i(\gamma_a) \otimes m_j(\gamma_a) = \sum_{\gamma_b \cap \gamma_c = \gamma_a} m_i(\gamma_b) m_j(\gamma_c) \qquad \forall \gamma_a \in \Gamma(\Omega) \tag{5}$$

The fact that $m(\emptyset) > 0$ can be explained in two ways: the open world assumption and the quantified conflict. The open world assumption, made by Dempster, reflects the idea that the frame of discernment must contain the true value. Necessarily, if the open world assumption is true, then the set of hypotheses must contains all possibilities. Under this interpretation, being $\emptyset$ the complement of Ω, the mass $m(\emptyset) > 0$ represents the case where the truth is not contained in Ω. The second interpretation of $m(\emptyset) > 0$ is that there is some underlying conflict between the sources that are combined in order to produce the BBA. Hence, the mass assigned to $m(\emptyset)$ represents the degree of conflict. In particular, it can be computed as follows:

$$m_i(\emptyset) \otimes m_j(\emptyset) = 1 - \sum_{\gamma_a \in \Gamma, \gamma_a \neq \emptyset} \left(m_i(\gamma_a) \otimes m_j(\gamma_a) \right) \tag{6}$$

4.3 DATA FUSION PROBLEM IN NETWORKED CONTEXT

Consider a network of multi-agents, which in our case might represent individual sensors or infrastructure, described by an indirect graph $\mathcal{G} = \{V, E\}$, where $V = \{v_i, i = 1, \cdots, n_V\}$ is the set of nodes and $E = \{e_{ij} = (v_i, v_j)\}$ is the set of edges represented by the pair of nodes incident on arc. This edge indicates a channel of communication between the couple of nodes. Edges are indirect and thus the existence of the arc e_{ij} implies the existence of the edge e_{ji}.

In this Chapter, we assume that no central unit is available to perform the aggregation in a centralized manner. The communication between different nodes is limited to the neighbours of the node under consideration, i.e., nodes physically (or directly) interconnected to the considered one. These assumptions are reasonable for the data fusion problem in the field of sensor networks or in the context of critical infrastructures.

A direct consequence of this assumption is that the rule of composition proposed by Smets cannot be used as it is. This is due to the fact that the application of this operator more than once over the same

Table 1: BBA assignments for the cause classification problem in a telecommunication network

Set	node 1	node 2	node 3	m_{12}	m_{123}
$\emptyset$	0.0	0.0	0.0	0.44	0.77
{a}	0.1	0.5	0.7	0.11	0.095
{b}	0.8	0.4	0.2	0.44	0.134
{a,b}	0.1	0.1	0.1	0.01	0.01

BBAs lead to different outputs. Note that, this could easily happen in a distributed context where the communication is local and limited to the one-hop neighbours. Now, since we are interested to a data fusion approach for which the result is not influenced by the sequence of messages exchange an alternative technique must be considered. For this reason, the approach proposed in [40] will be described in the next section.

To better understand this problem, let us consider a simple example of cause identification in a telecommunication network: in case of many delays in packet transmission, it is necessary to understand if a temporary congestion or a malicious attack is happening. Some sensors, like Intrusion Detection Systems (IDSs), could detect a Denial of Service (DoS). The United States Computer Emergency Readiness Team (US-CERT) defines the DoS attack as activities that render a component unusable or unavailable. A resource tied up for 100%, whether CPU, memory or bandwidth, will cause a DoS. The DoS attack can also lead to problems in the network "branches" around the actual computer being attacked. If the attack is conducted on a sufficiently large scale, entire regions can be compromised.

Note that, although a suitable way to define a BBA is usually problem dependent, a possible (general) way to define a BBA's allocation is to consider the reliability of information source. Suppose that data obtained from the source itself support a set of hypotheses in Ω. The subset γ_a of the power-set $\Gamma(\Omega)$, containing the set of hypotheses, will receive a mass $m(\gamma_a)$ value equal to the reliability of the source; $1 - m(\gamma_a)$ will be assigned to the universal set because no other information is available. Note that assigning a mass to the universal set means that we have no idea about the right hypothesis.

In Table 1, the centralized approach is shown. In this example, we consider a telecommunication network. Within this network, a congestion is happened and we can obtain information from three sources in order to find the probable cause of congestions. The table 1 shows not only the different values of BBAs assigned to different network nodes, but also some outputs. The frame of discernment is

$\Omega = \{a, b\}$, where a is the denial of service, i.e. the congestion of one or more network nodes in a conscious manner to harm some users of the telecommunications network, and b indicates congestion in telecommunication network because of the reprogramming of some router or network routing problems.

If we assume that node 1 is working with the node 2, by applying the Smets operator: the result is $m_1 \otimes m_2 = \{0.44, 0.11, 0.44, 0.01\}$. Then if the node 1 communicates with node 3, by exchanging information regarding the possible cause of the malfunction, the result will be $m_{12} \otimes m_3 = \{0.77, 0.095, 0.134, 0.001\}$. This is the result would be achieved by a centralized aggregation.

Now, if the communication is between the node 1 and node 3, by applying straightforwardly the Smets operator, the result is different from the one obtained in the centralized system. The application of Smets operator to masses obtained from the last interaction and ones assigned to node 1 has generated the result $m_{123} \otimes m_3 = \{0.8828, 0.0767, 0.0404, 0.0001\}$. If the decision on the cause fault has to be made, in the latter case there is a change of opinion, according to the latest aggregations: the cause is *a*, the Denial of Service, instead of the congestion hypothesis.

As previously stated, it can be noticed that the rule of combination proposed by Smets cannot be directly used in a distributed data aggregation context. In the next section we analyse the choice, introduced in [40], of a distributed algorithm able to update in a decentralized manner the knowledge of agents, for all nodes in the network.

4.4 DATA FUSION ALGORITHM IN NETWORKED CONTEXT

The algorithm proposed in [40] by Gasparri et al. allows to divide the knowledge of each agent in two parts: one is the piece of information shared between the two nodes, and the other is the innovative part of the information carried by the allocation of each node.

The decentralized algorithm is based on some assumptions. The network is described by a graph indirect $\mathcal{G} = \{V, E\}$. Communication between agents is asynchronous that falls into the gossip category, as shown in [13]. It is also necessary to build a spanning-tree $\mathcal{T} = \{V, \widehat{E}\}$, where $\widehat{E} \subseteq E$ and make it available to agents. The construction can be done as shown in [17]. Agents must be able to save data.

The proposed algorithm is of a gossip one and it is defined by a triplet $\{\mathcal{S}, \mathcal{R}, \mathbf{e}\}$, defined as:

- $\mathcal{S}$ is the set of local states of each agent in the network;
- $\mathcal{R}$ is local interaction rule that, for every pair of agents (i, j) such that $e_{ij} \in E$, it holds that

$$\mathcal{R} : \mathbb{R}^q \times \mathbb{R}^q \to \mathbb{R}^q$$

where q is the number of elements called *focal sets*;

- **e** is the process of edges selection for which $e_{ij} \in E(t)$ is the selected edge at time instant *t*.

The proposed algorithm is as follows.

Gossip Algorithm
Data: $t = 0$, $s_i(t = 0)$, $\forall i = 1, \cdots, n$
Results: $s_i(t_{end})$ $\quad \forall i = 1, \cdots, n$

while *end_condition* **do**
Select an edge $e_{ij} \in E(t)$ according to **e**;
Update the states of the selected agents applying the operator $\mathcal{R}$:

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

Let $t = t + 1$
end

To define the operator $\mathcal{R}$ is first necessary to introduce the operator $\odot$. Consider two sets of BBAs, defined as $m_k = \{m_k(\gamma_a) : \forall \gamma_a \in \Gamma(\Omega)\}$ and $m_i = \{m_i(\gamma_a) : \forall \gamma_a \in \Gamma(\Omega)\}$, so that is true $m_k = m_i \otimes m_j$. It then defines the operator $\odot$ as:

$$m_j = m_k \odot m_i \triangleq \tilde{m}_k^i \tag{7}$$

By starting from the element of the power set with higher cardinality and moving to the elements with lower cardinality, the value of a BBA can be computed recursively as follows:

$$m_j(\gamma_a) = \frac{m_k(\gamma_a) - \sum_{\gamma_b \cap \gamma_c = \gamma_a, \gamma_a \subset \gamma_b} m_j(\gamma_b) m_i(\gamma_c)}{\sum_{\gamma_a \subseteq \gamma_b} m_i(\gamma_b)} \tag{8}$$

It is now possible to introduce the operator $\mathcal{R}$, denoted with $\oplus$ to aggregate BBAs of the nodes as follows:

$$m_i(t+1) = m_j(t+1) = m_i(t) \oplus m_j(t) = \tag{9}$$
$$\{\Big(\tilde{m}_i^j(t, \gamma_a) \otimes \tilde{m}_i^j(t, \gamma_a)\Big) \otimes \bar{m}_{i,j}(t, \gamma_a),\ \forall \gamma_a \in \Gamma(\Omega)\}$$

where the element $\tilde{m}_i^j(t, \gamma_a)$ indicates innovation of agent *i* with respect to the agent *j* that can be calculated recursively using the operator $mathcal S$ as:

$$\tilde{m}_i^j(t, \gamma_a) = m_i(t, \gamma_a) \odot \bar{m}_{i,j}(t, \gamma_a) \tag{10}$$

and the element $\bar{m}_{i,j}(t, \gamma_a)$ is the common knowledge, i.e. knowledge exchanged between the two agents *(i,j)* after the last aggregation, set to the neutral element before the first TBM aggregation, i.e.

$$\bar{m}_{i,j}(t, \gamma_a) = \mathbf{n} = \{0, 0, \cdots, 0, 1\} \tag{11}$$

In Gasparri et al. [40], it is shown how this algorithm converges to the same result obtained by means of a centralised aggregation. The convergence time of the distributed algorithm is related to the diameter d of the spanning tree.

The computational complexity of the $\mathcal{R}$-operator is the same as the Smets' operator, in fact at each interaction two manipulation of the BBAs are carried out and their computation complexity is comparable to the application of the Smets operator.

In the next section the case study is presented with some results.

4.5 APPLICATION SCENARIO

The application of the TBM mainly consist of modeling the problem, building the frame of discernment and choosing the of assigning BBAs. The assignment of a BBA is usually problem dependent and significantly depends upon the source of information and knowledge of the system. In this work, we assume that some experts have provide a way to assign BBAs. Other possible approach can be found in [19, 95], where it has been considered not only the reliability of information sources but also the effect of mass assignment on the compound hypotheses.

As an application scenario, consider the case of n interconnected infrastructures on which we are able to obtain BBA, about the possible causes generating a critical event. All facilities have information regarding the events, but data are generated from different sources of information.

Facilities are made up of a supervisor who controls the system by acquiring data about the system and then sending changes back to the system for optimization. SCADA systems integrate data from a large number of remote locations. The data are concentrated and acted upon by some sort of logic processing at control centre, as the centralized TBM previously mentioned.

Communications between the control center and the elements of the field is carried out through a telecommunications network that may be proprietary, and thus with specific protocols created by producer itself, or as is happening increasingly often, by also using public Internet protocols.

The same channels, especially Internet, could be used to share information among infrastructures, for example the possible cause of failures. In smart cities field, the communication can be exchanged

Table 2: BBA assignments for each of five agents.

Set	Node 1	Node 2	Node 3	Node 4	Node 5
∅	0.0	0.0	0.0	0.0	0.0
{a}	0.3	0.0	0.0	0.0	0.2
{b}	0.3	0.4	0.1	0.4	0.4
{c}	0.0	0.4	0.5	0.4	0.1
{a,b}	0.3	0.0	0.0	0.0	0.0
{a,c}	0.0	0.0	0.0	0.0	0.0
{b,c}	0.0	0.0	0.3	0.0	0.0
{a,b,c}	0.1	0.2	0.1	0.2	0.3

also using other facilities as the power grid. This connection usually is realized by means of control centres and SCADA systems.

The idea to share information, generating common knowledge, can lead to avoid or prevent cascading or domino effects also for infrastructures still not involved in the fault. Information has to be exchanged and all nodes need to reach the same knowledge.

We consider $n = 5$ interdependent critical infrastructures and several failures take place within these facilities. Each infrastructure is able to define a BBA assignment, due to basic sensor information. BBAs have to be aggregated and shared among all infrastructures, to understand fault cause. The frame of discernment is $\Omega = a, b, c$, where a indicates a possible intrusion of cyber type [35], b indicates the failure of the isolated single unit in question and c is a possible natural disaster like an earthquake.

Table 2 includes the different values of BBA, obtained by five considered nodes. If you apply the algorithm on centralized sources of information, the result is shown in Table 3. In Table 3, each column is the result of Smets' operator: the first column is the combination between node 1 and node 2, the second column is the aggregation of the last result and the node 2 assignment, and so on.

Now, consider the distributed approach. First of all we decide the edges selection shown in Table 4. In Table 5, the output of the $\mathcal{R}$-operator is depicted. Each column is the aggregation of the the two nodes, related to the time step edge.

After each exchange of knowledge between two node, applying $\mathcal{R}$-operator, the two nodes have the same value of knowledge that is the output of the operator. So since $t = 5$ the nodes 4 and 5 contain the same value as $\{0.6334, 0.0541, 0.3070, 0.0125, 0.0014, 0.0, 0.0004, 0.0001\}$.

Table 3: Output of centralized TBM with incremental aggregations.

Set	Node 12	Node 123	Node 1234	Node 12345	C-TBM
$\emptyset$	0.36	0.468	0.5304	0.6334	0.6334
{a}	0.18	0.108	0.0648	0.0451	0.0451
{b}	0.34	0.346	0.3676	0.3070	0.3070
{c}	0.04	0.046	0.0308	0.0125	0.0125
{a,b}	0.06	0.024	0.0048	0.0014	0.0014
{a,c}	0.0	0.0	0.0	0.0	0.0
{b,c}	0.0	0.006	0.0012	0.0004	0.0004
{a,b,c}	0.2	0.002	0.0004	0.0001	0.0001

Table 4: Temporal edge selection.

Time	t=1	t=2	t=3	t=4	t=5	t=6	t=7
Edge	e_{12}	e_{23}	e_{34}	e_{45}	e_{34}	e_{23}	e_{12}

Then also all the other nodes reach the same values at time step $t = 7$, according to the centralized TBM outputs, see Table 1.

Note that, the stopping condition for the algorithm can be obtained according to [40] (Lemma 4), once the nature of the edge selection process is known.

4.6 CONCLUSIONS

The approach described in this Chapter is innovative in the field of Situational Awareness. The idea to extend the Transferable Belief Model in a de-centralized context is very helpful and productive , especially in the field of critical infrastructure's failures assessment , where the centralization of the computation is a counter-productive approach.

It is clearly a good step forward to integrate a situational awareness engine with the distributed monitoring and control of a network of infrastructures. They share, indeed, the same data coming from the filed, and leveraging such information can lead to a significant improvement of resilience and robustness. For example, in the case of a cyber attack, data coming from Intrusion Detection Systems (IDSs) and from standard measurements field sensors, can be combined in a distributed situational awareness with the flexible techniques and methodologies shown in the paper, to help both security staff to de-

Table 5: Distributed TBM.

Set	$\mathbf{s_1 \oplus s_2}$	$\mathbf{s_2 \oplus s_3}$	$\mathbf{s_3 \oplus s_4}$	$\mathbf{s_4 \oplus s_5}$	$\mathbf{s_3 \oplus s_4}$	$\mathbf{s_2 \oplus s_3}$	$\mathbf{s_1 \oplus s_2}$
$\emptyset$	0.36	0.468	0.5304	0.6334	0.6334	0.6334	0.6334
{a}	0.18	0.108	0.0648	0.0451	0.0451	0.0451	0.0451
{b}	0.34	0.346	0.3676	0.3070	0.3070	0.3070	0.3070
{c}	0.04	0.046	0.0308	0.0125	0.0125	0.0125	0.0125
{a,b}	0.06	0.024	0.0048	0.0014	0.0014	0.0014	0.0014
{a,c}	0.0	0.0	0.0	0.0	0.0	0.0	0.0
{b,c}	0.0	0.006	0.0012	0.0004	0.0004	0.0004	0.0004
{a,b,c}	0.2	0.002	0.0004	0.0001	0.0001	0.0001	0.0001

tect the attack, and control room staff to safer operate the infrastructure.

The proposed solution has the same advantages of the traditional TBM in terms of capability to deal with uncertainties, and the same disadvantages,e.g., exponential growth of the computational complexity with respect to the number of hypotheses.

In particular, the described algorithm relies on the hypothesis that a spanning tree can be computed, that is the network topology over which the data fusion is carried out is assumed to be a tree. Nevertheless, an extension of this approach to the case of more complex graph topologies has been proposed in [36].

5 AN AGILE MODEL FOR SITUATION ASSESSMENT

A relevant issue felt in the domain of Situation Awareness is related to the definition of models describing situations and threats of interest. Actually, the widely adopted approaches are based on two phases: employ training data as input of learning algorithms, and then validate the built model through other sets of data, gathered from the field. Model construction is therefore considered as an off-line process, and model correction is contemplated in terms of little adjustments in real-time applications. Agile models needs to evaluate also inconsistencies, contractions and error models, or re-define the entire model thanks to user informations.

In particular, the analysis is conducted with regard to the Evidence Theory approach. This method is usually applied in static classification problems, where time is not take into account, as in image processing. Evidence Theory starts from a set of exhaustive and exclusive situations and computes the power set. Then on the power set, belief and plausibility measures are evaluated. This technique contemplates automated reasoning on time-independent models and it is therefore addressed to static pattern recognition, in the domain of Situation Awareness. The mathematical formalism is the Transferable Belief Model, defined by Smets, able to simply identify modelling disagreements or deviations among several information sources.

This Chapter investigates about possible metrics to adopt in the correction process. Firstly, we shown the classical model inability to identify two following situations. We propose an algorithm using information regarding contradictions, to allow the model to be aware of different situations and to change opinion respect to previous pattern recognition. Some experimental results are shown related to a simple case study in the Critical Infrastructure domain are reported.

5.1 KNOWLEDGE REPRESENTATION FOR SITUATION AWARENESS

Within the context of Information Fusion, a capability required to automated reasoning systems is to understand relations among objects of interests and to assess the threats they could cause. This capability, together with others related to the data-fusion domain [55], is well defined as Level 2 and 3 of the Joint Directors of Laboratory (JDL) model, i.e. Situation Assessment and Threat Assessment, also referred to as Situation Awareness. In particular, the aim of Information Fusion theory is to define a framework of algorithms and techniques for systems able to support human operators in the decision making process, when huge quantity of heterogeneous data are available and must be correlated. Once the objects of interest in a certain domain have been detected and classified (JDL Level 1 - Object Refinement), the goal of Level 2 and 3 is to help the user to become aware of the on-going situation and related threats. JDL Level 4 is dedicated to the refinement of the inference process performed in Levels 1, 2 and 3, while, the recently introduced Level 5, *User Refinement*, contemplates the intervention of the user in the inference process [90].

Since the Information Fusion Theory has gained relevance, many approaches have been studied to perform inference, starting from rough data as Probabilistic Bayesian Networks [19], Evidence Theory [83], Neural Networks [34] and Markov Models [18]. Each of the mentioned approaches allows to classify and recognize situations and threats, previously modeled in a proper way, employing even uncertain and imprecise information gathered from the field. In particular, depending on the empirical structure of the knowledge, different models and inferring techniques suit better to represent the domain of interest: for example, hierarchical knowledge is well represented by cause-effect Bayesian Nets; flat and time-independent knowledge can be managed with Evidence Theory models; time-dependent patterns are well recognized by Markov Models; finally, complex, non-linear systems can be modeled by Neural Networks.

All the mentioned techniques have the idea to model the reality in a previous step, usually off-line. Then the model is applied in real application, thanks to the data gathered from the studied reality. The obtained model has the ability to work only for the particularly case for which has been created. The model can be only tuned in some parameters during the on-line mode. We think that a model should be tested also in real-time context where data can be changed during time for some reasons, as environment changes. The model should be also "agile" in order to evaluate reshaping informations. By this way, the model can be obtained also with not perfect knowledge of the complete system, and in future the model can be able to learn from its experience. The idea is to determine metrics to express changes in the input data in order to evaluate other output situations.

In order to measure the effectiveness of Information Fusion systems, several studies have been conducted to define metrics for each of JDL levels, see [11] and [92]. In general, the following metrics are identified for the Situation Awareness evaluation: *timeliness*, *confidence*, *cost*, *accuracy*, *throughput*. The evaluation of each metric is not trivial, as well as the definition of the best practice to adopt once the metrics have been computed (e.g. if the accuracy of a system is low, how is it possible to improve it?). In several works model refinement is regarded as an off-line task for human operators, as in [41]. Metrics evaluation usually requires the comparison between inferences elaborated by the system and reality. This kind of comparison is possible only in off-line validation processes and not in real-time operations, when reality is not known and must be assessed. For these reasons, the mentioned metrics are not suitable for real-time evaluations of the system; such kind of metrics cannot relay on reality, but must take into account only the intrinsic characteristics of the model itself.

In this Chapter, we take into account Evidence Theory, as a simple technique to score different situations. Smets' Transferable Belief Model is a mathematical representation of the Evidence Theory related by the concept of belief measures. This method allow the user to scoring different situations thanks to some information, called "evidence". The method considers the uncertainty of the model, defining not a probability measure but an interval of confidentiality. This interval has as lower and upper bounds, respectively the belief and the plausibility measures. The great disadvantage of the Evidence Theory is the computational complexity due to the definition of the power set. The power set is the set of all possible subset of all the considered situations.

In this Chapter we focus on the crucial aspect of knowledge model definition and management. In particular, we assume that a model for a certain domain of interest is given (through learning algorithms or defined by experts), and we investigate about metrics able to highlight in real-time modeling errors and inconsistencies. We believe that it is of great importance for the user to understand as soon as possible that the knowledge model employed by the system is inadequate, so that model correction can be performed manually by the user or automatically by the system. Model correction techniques go beyond the goals of this work, therefore little considerations on the topic are provided. Main focus is on the knowledge model employed Evidence Theory, characterized by a flat structure, suitable for classification of static situations and threats. Results of experimentations are reported, to show characteristics and inference results and define metrics for real-time model effectiveness evaluation.

To our knowledge, in literature problems of real-time model correction and metrics have been address in different works, but from a different perspective. In real time learning, it is contemplated the

definition of an initial model and its upgrading through real-time experiences in real world. In this approach, if the initial model defines few and simple actions, there are good chances that its validity is granted and modeling errors unlikely occur. Despite this, simple initial models need huge real-time adjustments before being effective, and in the meanwhile agent behaviour could seem inadequate. Complex initial model definition requires high initial efforts, therefore the chance of modeling errors and inconsistencies is high. The advantage is fast availability of effective models for real world operations and few real-time adjustment requirements. In summary, the complexity of the initial model in real-time learning algorithms should be a trade off between the mentioned aspects.

In [23], [96] and [58], are proposed different learning algorithms to build Markov Models, describing respectively a strategic game, automata behaviour and a generic dynamic system. All approaches are focused on the learing strategy that does not count on an initial model, therefore the problem of model validation is not taken into account.

In [38] and [15] is discussed the problem of repairing incorrect knowledge after off-line model construction. Despite our work, model correction is performed off-line and is based on the analysis of inconsistencies in the learnt model. Once inconsistencies are identified, they are corrected or inserted in the model as exceptional cases, so that the final model provided to the inference system is coherent and well-defined.

Another research domain that could be correlated to the study proposed in this Chapter is related to *anomaly detection*, in fact an anomaly can be regarded as a mismatch from a given model. The common approach adopted in this field and also in [74], is to define off-line a model for normal situations and a different model for abnormal situations, so that in real-time operations, anomalies can be recognized as well as normal situations. The need for abnormal behaviour models arises to avoid that real-time false alarms are generated each time that discrepancies with the models occur. Works in anomaly detection field mainly focus on off-line abnormal model definition techniques, despite of the proposed study whose goal is to highlight in real-time a mismatch between world representation and the on-going situation. The mismatch could occur even between reality and an abnormal behaviour model, suggesting modeling errors even in anomaly representation.

5.2 EVIDENCE THEORY APPLIED TO SITUATION AWARENESS DOMAIN

The term *Evidence Theory* was coined by Shafer in [83], reinterpreting the work of Dempster [22] on how to represent and aggregate epis-

temic uncertainty. Epistemic uncertainty and random uncertainty are usually considered as distant and antithetic concepts. Random uncertainty is generally related to variations of the physical system or the environment, e.g., the variations in weather conditions or in the life of a compressor or turbine. Epistemic uncertainty, on the contrary, is mainly related to the lack of knowledge concerning the quantity, the system processes or the environment, and is characterized by an high degree of subjectivity and vagueness. Classical example are the qualitative knowledge of a process or the lack of understanding of complex physical phenomena. However the probability can be seen as a particular case of belief [83], hence both aspects can be captured within the framework.

Evidence Theory [83] found its application in the domain of Situation Awareness [88], as a framework to classify static, time-independent patterns of situations. The approach consists in putting in relation evidences gathered from the field with causes that could have generated those evidences. Each time evidences are acquired, the set of possible causes becomes smaller and smaller, until the identification of the most plausible one. Evidences can be heterogeneous and even asynchronous, and they can be threaten also as fuzzy variables [10].

In the rest of this section Evidence Theory knowledge model characteristics and inference algorithms are presented.

5.2.1 *Knowledge Representation*

Knowledge model employed in Evidence Theory is typically characterized by a flat structure that can be represented as a bipartite graph $G = (\Omega, \Phi, \Lambda)$, see Figure 28, where:

- Ω represents the set of situations to be classified and that should be mutually exclusive and exhaustive;
- Φ is the set of evidence that can be gathered from the scenario;
- Λ contains direct edges in the form $(\omega_i; \phi_j)$, where $\omega_i \in \Omega$ and $\phi_j \in \Phi$.

Edges express correlation between situations and evidences. When specific evidence is acquired from the field, the corresponding situations are supported. In Evidence Theory, model structure is assumed to be fixed, that is why time dependent patterns cannot be represented.

As exemplification, let $\Omega = \{\omega_1 \cdots \omega_n\}$ be a finite set of possible values of a variable ω, where the elements ω_i are assumed to be mutually exclusive and exhaustive (e.g., different positions, different behaviors, different situations, etc.). Suppose that only vague evidence is available in order to distinguish between the different values; for instance, during a crime investigation, a witness has seen a long haired

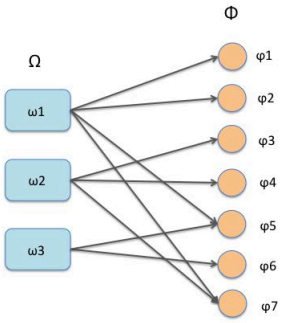

Figure 28: Evidence Theory knowledge model

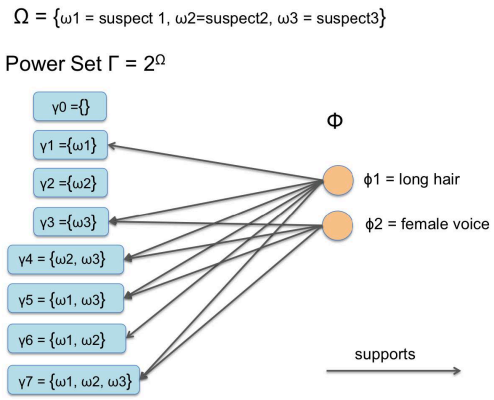

Figure 29: Evidence Theory model example

subject in the nearby of the crime scene, while another witness has heard a female voice. These two observations apply to subsets of the suspects, and there is the need to compose them in order to determine the guilty. From a set theoretical point of view, this means that, for each observation, a value is assigned to the corresponding subset of suspects, and these values are composed for the single suspect by considering the value associated to all the subsets of the suspects that contain that specifc person. Note that, in principle, all the subsets of the suspects have to be considered, and the resulting set, namely *Power Set*, has a number of elements that is exponential in the number of suspects. Specifically, if the generic subset of suspects is denoted as γ_i, the power set originated by the set Ω, is denoted by Γ or 2^{Ω} and is defined as $\Gamma = \{\gamma_1 \cdots \gamma_{|\Gamma|}\}$, and contains every subset $\gamma_i \subseteq \Omega$, see Figure 29. In this framework, the focus is on quantifying the belief of propositions of the form: *the true value* ω *is contained in* γ_i.

5.3 NOTES ON EVIDENCE THEORY AND INFERENCE ALGORITHM

In this section, mass distribution on the knowledge model, during real-time evidence acquisition, is discussed. The analysis of mass distribution characteristics leads to the identification of metrics that can be employed to improve Situation Awareness process.

5.3.1 *Unability to discriminate situations*

First matter taken into account is related to the capability of evidences contemplated in the model to discriminate situations of interest. For example, if the goal of a system is to classify a military platform and the only evidence taken into account by the model is velocity measurement, the system could be able to distinguish between an aircraft and a wheeled means of transport, but it probably will not be able to discriminate between a car and a motorbike. This kind of incapacity in classification, could be due to:

- The lack of evidences available from field sensors;
- A wrong knowledge model.

The effect of such a kind of ineffective classification at run-time is that the inference algorithm posts great part of mass, and consequently belief, on a not-atomic subset, $\gamma_i : |\gamma_i| > 1$, of the power set Γ.

When a model is well-defined and evidences gathered are sufficient to classify situations of interest, as well as new evidences are acquired, the mass distribution converge towards an atomic subset of the power set. If this does not happen, and mass distribution converge towards a non-atomic subset, it means that one of the two mentioned cases are occurring.

Indeed, if a model cannot distinguish between two or more situations, it is easily recognizable as their support is represented exactly by same evidences. In this case, it is worth to re-analyse knowledge about the domain of interest.

5.3.2 *Mass re-allocation*

If the model is running in on-line mode, a way to consider change of data is a mass re-allocation. The contradiction is represented in the mass of empty set. The universal set mass is the index of the completely ignorance obtained by data.

In this Chapter we consider the Smets framework at each step. The data aggregation is realized with the new data coming from the field, and the last outputs generated from the Evidence Theory model.

The results obtained are affected by the previous knowledge generated by past evidences. The idea is to move all the mass from the

empty set to the universal one. In this way, at each step, new situations inside the model can be considered.

5.3.3 *Closed world vs Open world assumption*

A very strict assumption in Dempster-Shafer formulation is that situations of interest must be exhaustive and mutually exclusive. Building such a kind of models is very difficult, if not impossible, unless to restrict automated reasoning to a small and well-known domain, where the closed world assumption is feasible. The closed world assumption states that all possible situations are modeled and that any other situation cannot exist.

In order to avoid such a strict and not realistic assumption, Smets introduced the *empty set* $\emptyset$ among plausible subsets of the power set Γ. In Smets formulation, the empty set mass is directly dependent on conflictual evidences acquired from the field: if $m(\emptyset) > 0$

- It might mean that there is some underlying conflict between the sources that are combined, in order to produce the BBA m;
- The open world assumption is supported: Ω might not be exhaustive, i.e., it might not contain all the possibilities. Under this interpretation, being $\emptyset$ the complement of Γ, the mass $m(\emptyset) > 0$ represents modeling errors, signifying that the truth might not be contained in Ω.

The mass of the empty set can be computed as follows:

$$m_{ij}(\emptyset) = 1 - \sum_{\substack{\gamma_a \neq \emptyset \\ \gamma_a \in \Gamma}} m_{ij}(\gamma_a) \tag{12}$$

If $m(\emptyset) > 0$, because of inconsistencies in evidences acquired up to that time, it might mean that:

- There are problems in sources gathering evidences: for example, one of the source produces wrong output measures;
- The situation observed evolves with time: for example, in time interval $[t_0, t_1]$ evidences acquired by the system correctly support a certain situation γ_i, then, when the situation evolves and becomes γ_j, new evidences gathered in time interval $[t_1, t_2]$, supporting γ_j, result to be in contrast with those related to $[t_0, t_1]$, and cause the empty set mass to increase and converge towards 1.

In the mentioned cases, the knowledge model the system refers to is correct, and the mass of the empty set increases because of malfunctioning sensors, or because the system reasons about time-dependent

situations, adopting a time-independent model. In this case, a solution to allow the system to classify a certain situation γ_i, and then correctly classify γ_j, without erroneously thinking that evidences are in conflict, is to transfer the empty set mass to the greater subset of the power set Γ, i.e. the one expressing the highest degree of ignorance (all values of Ω are plausible), so that the system can *change idea* about on-going observed situation.

Another reason explaining $m(\emptyset) > 0$ is that the knowledge model employed does not suit situations observed. In this case, transferring the empty set mass to the ignorance set does not lead to a correct classification of a new situation, but causes again the increase of $m(\emptyset)$. For what stated before, such a kind of cycles can be regarded as a metric to identify modelling errors and trigger learning process for real-time model correction.

5.4 TOWARDS AN ONLINE AUGMENTED IMPACT ASSESSMENT

Due to the increasing diffusion of Internet-based technology, the infrastructures, once separated and vertically integrated, are becoming more and more tightly interconnected and interdependent. There is then the need to provide a framework able to fuse the domain specific data at real time, in order to provide predictions with a wider perspective. This has been done in a recent European FP7 Project [1, 69, 70] by using data provided by the SCADA systems of the different infrastructures in order to provide a short-term prediction of the expected domino effects. However, although being potentially able to model several classes of failures such as earthquake or fire blast, each with its peculiar diffusion pattern and dynamics, relying on the SCADA system alone allows typically to notice only the effects of outages (e.g., a telecommunication node is down), without giving any insight on the causes.

The idea is to set up a framework for the identification of the causes that originated the failures and use such an information in order to evaluate the near-future evolution of the scenario (i.e., the domino effects and the degree of failure of a given infrastructure or subsystem). In fact, while a huge effort has been done to model the effects of specific failures such as fire blasts, terrorist attacks or cyber attacks, when interdependency models are used in a real time prospective [39, 69, 70], the only available data is the state of infrastructure components or subsystems which is typically “working" or “not working" (eventually a percentage of malfunctioning), without providing insights on the causes. Indeed, as one may expect, if a telecommunication node in a the telecommunication network is down due to a fire blast, the diffusion of failure will have a very different pattern with respect to the spread of a computer virus (i.e., in the case of fire nearby elements will be affected while in the case of computer virus

element with the same operating system will be affected). Hence, in order to use such frameworks at real time, the urge for a mechanism able to determine the cause is becoming mandatory.

Hence, a mandatory step is to provide insights on the causes of failure, in order to activate the corresponding dynamics in the interdependency model, which would not be "excited" otherwise; in fact, as said before, the SCADA system only provides the state of an element (i.e., it is aware of the effects), while in order to perform more refined analyses there is the need to assess the causes, which would influence the interdependency model in a very different way.

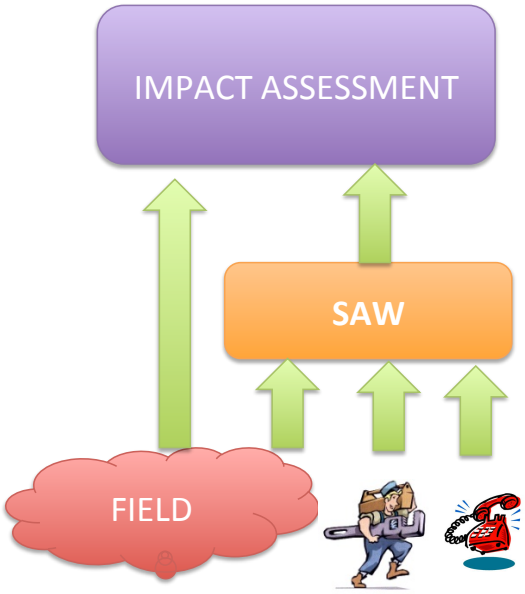

Figure 30: The proposed approach for integrating impact assessment via situation awareness

To achieve such a result a Situation Awareness (SAW) module should be interposed between the field and the Interdependency model, see Figure 30. Such a SAW layer is fed with the fields data, as well as with other information coming from different sources, such as customer or maintenance/recovery teams reports (i.e., unnoticed malfunctioning or blackout) and government or civil protection information (e.g., a tsunami warning). Such a use of SAW leads to an augmented impact assessment in which domino effects can be exploited, with their respective confidence levels. This implies also that the impact assessment should be done with a tool able to manage uncertainty.

One of the most desirable features of such a SAW modules, given the high degree of cyber interdependency among critical infrastructures, would be the ability to identify cyber-related failures [8, 76]. For cyber awareness, we refer to the user perception of detecting faults, generated by intrusions and, in general, cyber attacks. In fact, awareness is a process that leads to increased knowledge of the system, of the causes that generated failures and of the quality of services to

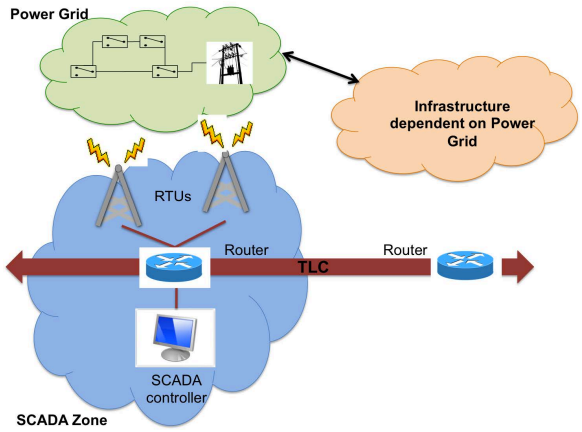

Figure 31: Case Study

customers. Hence, awareness helps to make decisions based on better knowledge of what is happening thanks to the integration of all available data. In the proposed architecture, the cyber awareness can be realized by means of Intrusion Detection and Prevention Systems, or by equipment, able to detect anomaly packet flows among SCADA telecommunication networks. These equipment send their outputs to SCADA control centre.

The impact assessment in Figure 30 is a block able to provide the impact evaluation on real equipment and services, after a fault or a failure. This module evaluates the cascading faults and domino effects of faults and failures on all interdependent infrastructures. This model has as inputs the data coming from the field and also outputs of the SAW module. These last data are uncertain, so it is important to consider input with uncertainty. A possible approach is fuzzy theory and especially fuzzy numbers. Among the others, CISIA (Critical Infrastructure Simulation by Interdependent Agents), [20, 72] is an agent-based simulator, using Triangular Fuzzy Numbers, to represent involved quantities. Indeed, this approach can realize the impact assessment module inside this framework.

5.5 APPLICATION IN CRITICAL INFRASTRUCTURE DOMAIN

In this section, a simple case study, driven from Critical Infrastructure domain, is presented as well as experimental results supporting previous considerations.

Consider the case study depicted in Figure 31: a power grid is controlled by a SCADA system through some RTUs. The connection between SCADA system and RTUs is granted by a telecommunication infrastructure. Another infrastructure (i.e. train transport system) depends on the power grid controlled by the SCADA.

We assume that 3 possible anomalies can be detected by 3 different intelligent sensors: alarms generated by the SCADA (X1), TLC net-

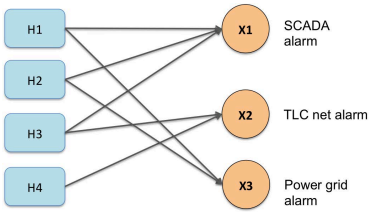

Figure 32: Case Study Model

work alarms (X2), power grid alarms (X3). The resulting anomaly vector is $v = [X1, X2, X3]$. For what concerns the causes, 4 events have been considered: power grid failure (H1), train transport system failure (H2), cyber attack to the telecommunication system (H3), telecommunication system failure (H4). The model for the case study presented is shown in Figure 32, and it is the bipartite graph $G = (H, X, E)$ where H and X are the set of 4 possible causes and 3 faults, respectively and E only contains direct edges in the form (h_i, x_j), where $h_i \in H$ and $x_j \in X$.

5.5.1 *First Example: the Right Behaviour of the Model*

Suppose that a cyber attack is going to occur. It causes the generation alarms from the SCADA and the telecommunication network. Suppose that after some time, the telecommunication alarm goes down as anomalous traffic that is no further detected and later also the SCADA alarm turn into normality thanks to operator service. The alarm vector at different time steps is the following one:

To: $v = [\alpha, \beta, 0]$
T1: $v = [\alpha, \beta, 0]$
T2: $v = [\alpha, 0, 0]$
T3: $v = [\alpha, 0, 0]$

where $alpha = 0.6$ and $\beta = 0.9$.

At each time step, Evidence Theory framework, implementing Smets rule for mass combination, is fed with the displayed alarms at the current time, and with the results of the last evaluation of the module itself. So at time T1, we combine the mass assignments of the time steps, due to $v = [\alpha, \beta, 0]$, and the result obtained at T0. Consequently, at time T2, we combine the mass due to alarm happened at time T2, $v = [\alpha, 0, 0]$, and the evaluations obtained at time T1.

In Table 6, mass assignment for the power set is shown, at each step time. It is possible to notice that the set {H3} is the one containing the higher value respect to the others. In fact, at time T2 and T3 the system increases the trust on {H3} as new data are acquired, confirming the evaluation performed by the system at previous time steps. Thus, the belief of the true is in {H3} increases, while the belief that it could

Table 6: Mass Assignment for the first example

	T0	T1	T2	T3
{∅}	0	0	0	0
{H1}	0	0	0	0
{H2}	0	0	0	0
{H3}	0.54	0.8316	0.9266	0.9647
{H4}	0	0	0	0
{H1, H2}	0	0	0	0
{H1, H3}	0	0	0	0
{H1, H4}	0	0	0	0
{H2, H3}	0	0	0	0
{H2, H4}	0	0	0	0
{H3, H4}	0.36	0.1584	0.0634	0.0253
{H1, H2, H3}	0.06	0.0084	0.0094	0.0097
{H1, H2, H4}	0	0	0	0
{H1, H3, H4}	0	0	0	0
{H2, H3, H4}	0	0	0	0
{H1, H2, H3, H4}	0.04	0.0016	0.0006	0.0003

be in other subsets decreases. the reader can notice that other subsets taken into account by the system at T1 include always {H3}.

5.5.2 *Second Example: the Wrong Behaviour of the Model*

In this example, consider at first a cyber attack, arising X1 and X2 alarms as in previous example, then, consider also an attack causing a failure on the power grid, as highlighted by alarm X3. The vector of anomalies is summarized as follows:

- T0: $v = [\alpha, \beta, 0]$
- T1: $v = [\alpha, \beta, 0]$
- T2: $v = [\alpha, 0, 0]$
- T3: $v = [\alpha, 0, 0]$
- T4: $v = [0, 0, \gamma]$
- T5: $v = [0, 0, \gamma]$

where $alpha = 0.6$ and $\beta = 0.9$ and $\gamma = 0.7$.

In Table 7, outputs of the example are shown,with regard to mass assignment. It can be noticed that until time step T3, as in previous example, the system is able to understand the cause of evidences

Table 7: Mass Assignment for the second example

	T0	T1	T2	T3	T4	T5
{∅}	0	0	0	0	0.693	0.9009
{H1}	0	0	0	0	0	0
{H2}	0	0	0	0	0	0
{H3}	0.54	0.8316	0.9266	0.9647	0.2894	0.0868
{H4}	0	0	0	0	0	0
{H1, H2}	0	0	0	0	0.007	0.0091
{H1, H3}	0	0	0	0	0	0
{H1, H4}	0	0	0	0	0	0
{H2, H3}	0	0	0	0	0	0
{H2, H4}	0	0	0	0	0	0
{H3, H4}	0.36	0.1584	0.0634	0.0253	0.0076	0.0023
{H1, H2, H3}	0.06	0.0084	0.0094	0.0097	0.0029	0.0009
{H1, H2, H4}	0	0	0	0	0	0
{H1, H3, H4}	0	0	0	0	0	0
{H2, H3, H4}	0	0	0	0	0	0
{H1, H2, H3, H4}	0.04	0.0016	0.0006	0.0003	0.0001	0.0000

gathered. As soon as the alarm X3 arises, Evidence Theory algorithm registers high conflict between previous evidences and the new one and assign big part of the mass to the empty set, reducing the mass of all other subsets. After some iterations, the algorithm is not any more able to identify the subset containing the truth, and it can only state that high contradiction among data has resulted.

Results of this example confirm that Evidence Theory does not suit dynamic pattern recognition problems.

To overcome this limit, we suggest to re-distribute the mass of the empty-set to the universal one, expressing the maximum ignorance on the true cause. Starting from the universal set, the mass can be spread on all possible subsets of the power set and the system can properly identify both causes, occurred one after the other. With this regard, inputs of the algorithm and mass redistribution at each time step are reported hereafter:

T0: $v = [\alpha, \beta, 0]$
T1: $v = [\alpha, \beta, 0]$
T2: $v = [\alpha, 0, 0]$
T3: $v = [\alpha, 0, 0]$
T4: $v = [0, 0, \gamma]$
T5: $v = [0, 0, \gamma]$
T6: mass re-distribution

Table 8: Mass Assignment for the second example, using the re-distribution approach starting from T5. Values for previous time steps are in Table 7

	T5	T6	T7	T8	T9
{∅}	0.9009	0	0.0624	0	0.0187
{H1}	0	0	0	0	0
{H2}	0	0	0	0	0
{H3}	0.0868	0.0868	0.0260	0.0260	0.0078
{H4}	0	0	0	0	0
{H1, H2}	0.0091	0.0091	0.6404	0.6404	0.8734
{H1, H3}	0	0	0	0	0
{H1, H4}	0	0	0	0	0
{H2, H3}	0	0	0	0	0
{H2, H4}	0	0	0	0	0
{H3, H4}	0.0023	0.0023	0.0007	0.0007	0.0002
{H1, H2, H3}	0.0009	0.0009	0.0003	0.0003	0.0001
{H1, H2, H4}	0	0	0	0	0
{H1, H3, H4}	0	0	0	0	0
{H2, H3, H4}	0	0	0	0	0
{H1, H2, H3, H4}	0.0000	0.9009	0.2703	0.3326	0.0998

T7: $v = [0, 0, \gamma]$
T8: mass re-distribution
T9: $v = [0, 0, \gamma]$

In Table 8 are shown the outputs of the algorithm from T5 to T9, considering that at time T6 and T8 the system applies mass re-distribution from the empty set to the universal one. The result is that the algorithm approach can also recognise dynamical pattern, as in Table 8. In fact at time T5 the highest value is associated to {H3} and at time T9 this value is related to {H1, H2}. The re-distribution of masses should be applied till the value of the mass of the empty-set is above a pre-defined threshold value.

5.5.3 *Third example: the Wrong Knowledge Model*

In this example, we consider an extension of the previous case: after the failure on the power grid, we suppose that another alarm cause X2 arising, while X3 is still persisting. So in these time steps, we have two faults simultaneously: a fault occurred in the power grid and one in the equipment of the telecommunication network. A possible cause

for both could be a fire, as it can destroy some branches of the power grid and also equipment that are in proximity to the fire.

The vector of anomalies is the following:

T0: $v = [\alpha, \beta, 0]$
T1: $v = [\alpha, \beta, 0]$
T2: $v = [\alpha, 0, 0]$
T3: $v = [\alpha, 0, 0]$
T4: $v = [0, 0, \gamma]$
T5: $v = [0, 0, \gamma]$
T6: mass re-distribution
T7: $v = [0, 0, \gamma]$
T8: mass re-distribution
T9: $v = [0, 0, \gamma]$
T10: $v = [0, \beta, \gamma]$
T11: mass re-distribution
T12: $v = [0, \beta, \gamma]$
T13: mass re-distribution
T14: $v = [0, \beta, \gamma]$

Also in this case, we apply the re-distribution algorithm at time step T11 and T13. The re-distribution algorithm can be applied if the value of the empty set is higher than a threshold value. For this reason at time T10, we does not execute the re-distribution algorithm: the value of empty set $\{\emptyset\}$ at T9, as 0.0187 is under the minimum threshold.

In Table 9 we show only last results of the algorithm. In this case the re-distribution of masses does not reduce the contradiction value as evidences gathered will always be in conflict with regard to the knowledge model employed, despite previous example.

In this case, transferring the empty set mass to the ignorance set does not lead to a correct classification of a new situation, but causes again the increasing of $m(\emptyset)$. For what stated before, such a kind of cycles can be regarded as a metric to identify modelling errors and to trigger learning process for real-time model correction.

One possible action to take in this cases is to modify the knowledge model employed as reference. In our example, the problem arises considering together X2 and X3 alarms. In fact the intersection of relative hypotheses of these alarms is the empty set. For this reason, a possible approach is to increase the frame of discernment, adding a new hypothesis H5. This hypothesis H5 is linked by two edges that go into X2 and X3 alarms. The new knowledge model is depicted in Figure 33. Let now consider the new knowledge model and the following vector of anomalies:

T0: $v = [\alpha, \beta, 0]$
T1: $v = [\alpha, \beta, 0]$

Table 9: Mass Assignment for the third example, using the re-distribution approach starting from T9. Values for previous time steps are in Tables 7 and 8

	T9	T10	T11	T12	T13	T14
{∅}	0.0187	0.8733	0	0.6575	0	0.6663
{H1}	0	0	0	0	0	0
{H2}	0	0	0	0	0	0
{H3}	0.0078	0.0024	0.0024	0.0007	0.0007	0.0002
{H4}	0	0	0	0	0	0
{H1, H2}	0.8734	0.0943	0.0943	0.0708	0.0708	0.0549
{H1, H3}	0	0	0	0	0	0
{H1, H4}	0	0	0	0	0	0
{H2, H3}	0	0	0	0	0	0
{H2, H4}	0	0	0	0	0	0
{H3, H4}	0.0002	0.0270	0.0270	0.2447	0.2447	0.2580
{H1, H2, H3}	0.0001	0.0000	0.0000	0.0000	0.0000	0.0000
{H1, H2, H4}	0	0	0	0	0	0
{H1, H3, H4}	0	0	0	0	0	0
{H2, H3, H4}	0	0	0	0	0	0
{H1, H2, H3, H4}	0.0998	0.0030	0.8763	0.0263	0.6838	0.0205

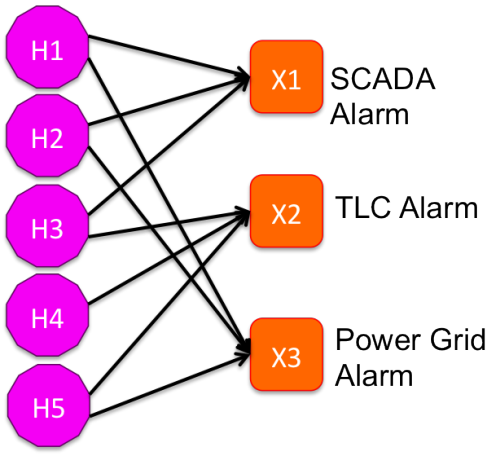

Figure 33: The new knowledge model, considering a frame of discernment of five hypotheses

T2: $v = [\alpha, 0, 0]$
T3: $v = [\alpha, 0, 0]$
T4: $v = [0, 0, \gamma]$
T5: $v = [0, 0, \gamma]$
T6: mass re-distribution
T7: $v = [0, 0, \gamma]$
T8: mass re-distribution
T9: $v = [0, 0, \gamma]$
T10: $v = [0, \beta, \gamma]$
T11: mass re-distribution
T12: $v = [0, \beta, \gamma]$
T13: mass re-distribution with new hypothesis in the knowledge model
T14: $v = [0, \beta, \gamma]$
T15: mass re-distribution with new hypothesis in the knowledge model
T16: $v = [0, \beta, \gamma]$

The mass re-allocation process is still necessary to allow the evaluation to evolve. As shown in Table 9 only applying the mass transferring is not enough to model possible causes occurring in the field. As soon as it is noticed that the empty set mass increses ad decreases with mass-redistribution, at time step T13, the new hypothesis H5 is introduced and, at T14, the higher value of mass is allocated on H5 hypothesis. The empty-set mass is reduced, and this is still true at time T16, after another execution of mass-reallocation and Evidence Theory. The label associated to H5 can be the fire explosion described in the initial part of the example, but in real-time context and with automatic procedures, identifying the meaning associated to H5 can be very difficult without the help of human operators.

Table 10: Mass Assignment for the third example, applying at T13 the new knowledge model. Values for previous time steps are in Tables 7 and 8

	T9	T10	T11	T12	T13	T14	T15	T16
{∅}	0.0187	0.8733	0	0.6575	0	0.2520	0	0.0650
{H1}	0	0	0	0	0	0	0	0
{H2}	0	0	0	0	0	0	0	0
{H3}	0.0078	0.0024	0.0024	0.0007	0.0007	0.0002	0.0002	0.0001
{H4}	0	0	0	0	0	0	0	0
{H5}	-	-	-	-	0	0.4142	0.4142	0.7512
{H1, H2}	0.8734	0.0943	0.0943	0.0708	0.0708	0.0089	0.0089	0.0009
{H1, H3}	0	0	0	0	0	0	0	0
{H1, H4}	0	0	0	0	0	0	0	0
{H1, H5}	-	-	-	-	0	0	0	0
{H2, H3}	0	0	0	0	0	0	0	0
{H2, H4}	0	0	0	0	0	0	0	0
{H2, H5}	-	-	-	-	0	0	0	0
{H3, H4}	0.0002	0.0270	0.0270	0.2447	0.2447	0.0805	0.0805	0.0244
{H3, H5}	-	-	-	-	0	0	0	0
{H4, H5}	-	-	-	-	0	0	0	0
{H1, H2, H3}	0.0001	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
{H1, H2, H4}	0	0	0	0	0	0	0	0
{H1, H2, H5}	-	-	-	-	0	0.0460	0.0460	0.0236
{H1, H3, H4}	0	0	0	0	0	0	0	0
{H1, H3, H5}	-	-	-	-	0	0	0	0
{H1, H4, H5}	-	-	-	-	0	0	0	0
{H2, H3, H4}	0	0	0	0	0	0	0	0
{H2, H3, H5}	-	-	-	-	0	0	0	0
{H2, H4, H5}	-	-	-	-	0	0	0	0
{H3, H4, H5}	-	-	-	-	0	0.1775	0.1775	0.1266
{H1, H2, H3, H4}	0.0998	0.0030	0.8763	0.0263	0.0263	0.0008	0.0008	0.0000
{H1, H2, H3, H5}	-	-	-	-	0	0	0	0
{H1, H2, H4, H5}	-	-	-	-	0	0	0	0
{H1, H3, H4, H5}	-	-	-	-	0	0	0	0
{H2, H3, H4, H5}	-	-	-	-	0	0	0	0
{H1, H2, H3, H4, H5}	-	-	-	-	0.6575	0.0197	0.2718	0.0082

5.6 CONCLUSIONS

This Chapter analyses a huge problem of the Evidence Theory: how to apply it in on-line context. The main enhancement respect to state-of-art is the mass-redistribution algorithm able to detect when the actual situation is different respect to the previous one.

Further analyses are mandatory in order to understand when the knowledge model of the case study is not enough in the actual situation and how to change it in an automatic way.

6

HIERARCHICAL STATE ESTIMATION FOR SMART GRIDS

State estimators are a crucial element of power networks and must be designed to be robust to bad or missing data. Recent work has yielded insights into the ability of centralised state estimators to malicious bad data injection, but does not extend to hierarchical or distributed state estimators. Conversely, work on distributed state estimators relies on linearisation affecting the model fidelity.

In this Chapter we therefore present a multi-level state estimator able to describe interconnected sub-networks linked by tie-lines. In addition to providing a strict hierarchical formulation we pay particular attention to the stability of the estimator and its ability to obtain rapid convergence in the presence of bad data, which is crucial both for malicious data and where state estimates have to be obtained in badly-partitioned sub-networks.

We describe our analysis of the state estimator sensitivity also in relation to decomposition and conditioning techniques, which result in trade-offs between stability and the ability to detect attacks and report validation results for the IEEE 118 Bus Test Cases.

6.1 INTRODUCTION

One of the principal objectives of developments in the smart grid area is the ability to operate all elements of the grid closer to their respective safety margins, thereby maximising the utility of resources whilst also enhancing efficiency. At the same time not only the integration of substantial renewable energy sources including from small generators such as individual home photovoltaic sources, but also of highly variable loads particularly in the form of electric mobility changes requirements for managing the smart grid. State estimation plays a crucial role in this.

We argue that enhancing the stability, robustness, and security of the smart grid is to be enhanced considerably by the development of hierarchical or distributed state estimators reflecting the more limited ability of centralised networks to observe and control all aspects of the grid in detail. Such hierarchical systems also enable fine-grained demand management and thereby further aid in increasing efficiency of modern grid systems.

This has been recognised for some time [94] and is the subject of on-going research [102] as novel types of network topologies and facilities make it highly desirable to obtain state estimation results not only in a single, centralised location. However, most such approaches have relied on a number of somewhat optimistic assumptions that may only be applicable in carefully-designed topologies. Clearly, however, one would wish to obtain such state estimates even for networks that do not exhibit large overlapping areas or where data is missing without having to sacrifice accuracy of the estimate.

This Chapter therefore reports a hierarchical state estimator, but one where we seek to minimise the additional requirements that must be imposed to only tie-lines. Just as importantly, however, we seek to characterise the fidelity of the model and link this to the overall robustness of the models.

As has been demonstrated recently by Liu *et al.*[57] and subsequent work such as [16], however, state estimators are susceptible to *malicious bad data injection*. However, research to date has concentrated on the problem of detecting and mitigating such malicious injection, which cannot be corrected by the same measures used for bad data resulting from random failures. In this paper we further argue that one of the key properties of a functional state estimator is the speed at which convergence is achieved and that this represents a separate but at least equally important attack objective in its own right. This, however, requires a more precise characterisation of the (hierarchical) state estimator than has been achieved so far.

6.2 STATE ESTIMATION

As both speed and robustness are critical in obtaining an estmate on the state of a power network, relevant algorithms must exhibit rapid convergence and be computationally efficient. The most widely used and accepted technique for this is the weighted least squares (WLS) approach.

This well-known and widely studied approach conducts an estimate on the n phase angle state variable vector $x = x_1, x_2, \ldots, x_n{}'$ based on the m active power measurements $= z_1, z_2, \ldots, z_m{}'$ where z is expressed as $z = h(x) + e$.

The term $h(.)$ is the function vector — usually a not linear function — and e is the independent measurement noise, which is assumed

to have a Gaussian distribution with zero mean value, and with covariance σ. We note that in the case of the static, centralised WLS approach, the number of measurements is significantly larger than the number of state variables, resulting in over-determined identification, which can be expressed as shown in equation 13 to quantify the measurement redundancy where n is the number of system variables (the bus number in our case) and m is the number of the available measurements.

$$\eta = \frac{m}{2n-1} \tag{13}$$

For these base measurements, we explicitly re-state common assumptions found in state estimator design and modelling that are obviously not taking deliberate attacks into account:

- The mean value is zero
- Measurement error are independent, hence $cov(e)$ is $\text{diag}\{\sigma_1^2, \sigma_2^2, ..., \sigma_m^2\}$

We will provide a further discussion of these assumptions and observations in section 6.4, but note that this aspects has been the focus of most existing work on malicious bad data injection [57, 52, 42].

The state estimation problem is usually solved as an unconstrained WLS problem. The WLS estimator minimizes the weighted sum of the squares of the residuals, expressed as

$$\begin{aligned} J(x) &= \sum_{i=1}^{m} \frac{(z_i - h_i(x))^2}{W_{ii}} \\ &= [z - h(x)]^T R^{-1} [z - h(x)] \end{aligned} \tag{14}$$

where $R = diag(R_i)$ is the weighting matrix. At the minimum, the first-order optimality conditions must be satisfied. This can be expressed as:

$$g(x) = \frac{\partial J(x)}{\partial x} = -H^T(x) R^{-1} [z - h(x)] = 0 \tag{15}$$

where H is the $m \times n$ measurement Jacobian matrix.

The first order necessary condition for a minimum are that

$$\frac{\partial J(x)}{\partial x} = -H(x)^T R^{-1} [z - h(x)] = 0 \tag{16}$$

Expanding the non-linear function $g(x)$ into its Taylor series around the state vector x^k results expressed into an iterative notation which depends on the iteration number value k and x^k represent the solution vector at iteration k.

The solution of the WLS problem is evaluated performing a back/-forward substitutions at each iteration k with respect to the variable Δx^{k+1} of the normal equation expressed below:

$$G(x^k)\Delta x^{k+1} = H^T(x^k)R^{-1}\left[z - h(x_k)\right] \tag{17}$$

where $\Delta x^{k+1} = x^{k+1} - x^k$.

In order to accomplish a very large scale monitoring of interconnected power systems, the multilevel SE idea has been introduced in [44] where it has been presented as a natural extension of the centralized WLS method (see e.g. [59]).

Several approaches to more decentralised state estimation have been proposed requiring iterative methods for sparse (linear) systems and efficient parallel algorithms, see e.g. [9] and [81].

In one of the earliest hierarchical models proposed by van Cutsem and Ribbens-Pavella [94], a *star-like* hierarchical state estimation was proposed.

Similar restrictions are also found in more recent work including by Gómez Expósito *et al.*[44]. Here, each area has its own state estimator performing local the state estimation and, according to the local full convergence approach, sends its results to a higher hierarchical layer. In this approach, the resulting network encompasses n systems sharing some border areas (noting that the same border areas could be shared between different system at the same time) where subsystems are adjacent. By expressing the hierarchical procedure approach as summarised above from [44], the same can be decomposed into n levels, where n represents the number of levels:

$$y_0 = f_1(y_1) + e_1 \tag{18}$$
$$y_1 = f_2(y_2) + e_2 \tag{19}$$
$$\vdots$$
$$y_{l-1} = f_r(y_l) + e_l \tag{20}$$

We observe that the general formulation 20 has the same form of [5] when $h(y) = f_1\left[f_2 \cdots (f_l(y_l))\right] \quad \Rightarrow \quad H(y) = \prod_{i=1}^{l} F_i(y_i)$, where H and $F_i, i = 1, \ldots, l$ representing the Jacobian matrices of h and $f_i, i = 1, \ldots, l$, respectively. Gómez Expósito *et al.*[44] also provide a detailed analysis of the possible scenarios in which the n-level model can be assumed as linear or nonlinear. We observe that in this approach, each level implies the solution of a WLS problem which, by generalising the whole procedure for the k-level version, we can summarise as follows:

LEVEL i: Obtain the $\tilde{y}_i$ satisfying

$$F_i^T G_{i-1}\left[\tilde{y}_{i-1} - f_i(\tilde{y}_i)\right] = 0 \tag{21}$$

by iteratively solving the associated normal equation

$$[F_i^T G_{i-1} F_i] \Delta y_i(k) = F_i^T G_{i-1} [\tilde{y}_{i-1} - f_i(y_i(k))] \tag{22}$$

The variable $y_i(k)$ is the estimated value of the state variables at step k at level i, and $\Delta y_i(k) = y_i(k+1) - y_i(k)$.

The hierarchical model described here (see also the recent survey by Gómez Expósito *et al.*[45]) as well as subsequent work by Korres [51] and Yang *et al.*[102, 103] requires a fixed structure. Recent work by Xie *et al.*claims to be *fully distributed* [101], without the need for a fixed control structure or indeed the requirement for local observability. This distributed approach can be summarised by the following properties:

- A multi-area power estimation system is partitioned into N regions, where each region n correspond to a non-overlapping control area. If necessary, each area may but is not required to exchange information with neighbouring areas. As a result, the measurement model for the multi-area state estimation is reconditioned as follow:

$$z_n = hn(x) + e_n \tag{23}$$

  where z_n is the measurement vector, which includes the boundary injection and flow measurements in the control area n.

- Global observability is assumed to be guaranteed and the gain matrix G is full rank.

The real distributed state estimation algorithm, called also $M-$CSE, is applied first to a linearised (DC state estimation problem formulation) by iterating the solution of the following problem:

$$x_n(i+1) = x_n(i) - \left[\beta(I) \sum_{l \in \omega_n} (x_n(i) - x_l(i)) - \alpha(i) H_n^T x_n(i) \right] \tag{24}$$

where $\alpha(i), \beta(i))$ are appropriately chosen time-varying weight sequence. The algorithm 24 is *distributed* since for the $n-th$ control area it involves only the data from the sensors in its neighbourhood ω_n. In the AC state estimation, which also uses the linearised Jacobian matrix H of the DC state estimation, the iterative equation 24 is modified to

$$\begin{aligned} x_n(i+1) = x_n(i) - a[b \sum_{l \in \omega_n} (x_n(i) - x_l(i)) + \\ -\alpha(i) \bar{H}_n^T (x_n(i))(\bar{z_n} - \bar{H_n})(x_n(i) x_n(i))] \end{aligned} \tag{25}$$

6.3 MULTI-AREA HIERARCHICAL STATE ESTIMATOR

The hierarchical multi-level, multi-area state estimator we are presenting in this section is an extension and improvement over the state estimator described in [44].

While in [51] the whole network is divided into n parts with the possibility of multiple partial overlapping between all sub-areas, our model utilises a non-overlapping approach. This means that the all sub-areas are interconnected to each others by means of tie-lines only.

The degree of overlapping between couple of area can change also depending on the coordination scheme adopted. Usually, three are the possible hypotheses described below:

NON-OVERLAPPING AREAS These have no bus and no branch in common; they are connected by tie-lines ending at border buses. Those tie-lines define the interconnection area

MINIMALLY OVERLAPPING AREAS These are adjacent areas overlapping over just one layer of border buses; there exist no tie-lines connecting two areas.

FULLY OVERLAPPING AREAS We can identify two possible sub-cases, namely tie-line overlapping areas sharing tie-lines and the corresponding border buses. Deep overlapping area share several layer of border buses.

The state estimator model that we present here relies on a hierarchical and nested structure which can be identified naturally as a *tree structure*.

A tree-structured graph is set of *points*, called nodes, and lines, called *edges*. In our model each node is a stare estimation process, and an edge is a information flow. A collection of nodes and edges, in order to be considered as a tree, must satisfy the following properties:

1. In each tree structure there is a node distinguished as the *root*. In our model, the root node is the highest level of the state estimation, usually defined as l level. The root node of a tree is represented as the top diagrammatically.

2. Every node c other than the root is connected by an edge to some other node p called the parent of c.

3. A tree is connected in the conventional graph-theoretic sense such that if we start at any node n other than the root, move to the parent of n, we eventually reach the tree's root.

In a multi-level approach is important to consider also a distributed environment, usually called *multi-area*, grouping in clusters the buses

and branches. As the case of overlapping areas has been covered extensively in the literature we here consider only the non-overlapping hypothesis.

In the case of non-overlapping areas, each bus in the system and the associated variables is assigned to one distinct area. Usually, these areas are separated by tie-lines, whose terminal buses belong to different areas. The definition of areas is arbitrary; in a real state estimation scenario these might follow simply geographical or organisational boundaries. We assume that each area will estimate its own state using the available local area measurements, any information arising from lower levels if the area itself is not at the leaf level of the tree structure, and information coming from higher level.

The hypothesis of fully and partially overlapping areas has been omitted as not realistic in the distributed smart grid context. This is due to the following reasons:

- Both total and the partial overlapping areas are created when the distribution network is static. In the case of a smart grid context, distribution areas may vary over time reconfiguring its topology according to dynamic requirements. This may make the inclusion of such areas no longer possible.
- With the previous premise, overlapping areas are no longer known in advance which, in terms of safety and robustness, represent a further problem. Not knowing which sub-areas are overlapping could result in an adversary being able to force the state of the entire system trivially by creating artificial, malicious overlapping regions resulting in either state changes induced by the attacker or loss of stability.

When solving the state estimation problem for individual areas, each are estimator will use measurements from its own area. However, there will exist boundary measurements, which will represent a function of state variables of both neighbouring areas. Therefore, within each area two types of variables can be distinguished:

border variables appearing in the measurement model of at least an adjacent area.

internal variables not involved in the measurement model of neighbour areas.

6.3.1 *K-level Hierarchical State Estimator Formulation*

The k-level multi-area state estimator can be represented naturally using a tree-structure as outlined above. The root is the main state estimator and is assumed to be highest level, denoted l. Each level i is

made up by r_i nodes, where each node is a state estimation involving the solution i of a WLS problem.

Each node has r_{ij} child nodes. Nodes without children are called *leaf nodes* and, in this proposed state estimator, these nodes are the nodes at the level 1. In this section, we provide only a compact form of the general k-level hierarchical state estimation algorithm as pseudo-code, but give a fully-elaborated instantiation for a two-level structure in section 6.3.2. Obtaining the estimate requires us to distinguish three cases (root, leaf, and intermediate levels):

MULTI-AREA LEVEL 1: Obtain the estimate $\tilde{y}_{1j}$ for each area S_j by iteratively solving the associated normal equations:

$$\left[F_{1,j_1}^T R_{1,j_1}^{-1} F_{1,j_1}\right] \Delta\tilde{y}_{1,j_1}(k) = \\ = F_{1,j_1}^T R_{1,j_1}^{-1} \left[y_{0,j_1} - f_{1,j_1}(y_{1,j_1}(k))\right] \tag{26}$$

$$\left[F_{1,b_1,j_1}^T R_{1,b_1,j_1}^{-1} F_{1,b_1,j_1}\right] \Delta\tilde{y}_{1,j_1}(k) = \\ F_{1,b_1,j_1}^T R_{1,b_1,j_1}^{-1} \left[y_{0,b_1,j_1} - f_{1,b_1,j_1}(y_{1,j_1}(k))\right] \tag{27}$$

The inputs of this level are the measurement vectors y_{0,j_1} and y_{0,b_1,j_1} and the Jacobian matrices F_{1,j_1} and F_{1,b_1,j_1}, besides the gain matrices at level 1 R_{1,j_1} and R_{1,b_1,j_1}. The Jacobians are updated at each iteration at level 1, due to the current value of $y_{1,j_1}(k)$ and y_{1,j_1,b_1}, but also when new values come from level 2, due to current estimation of $\hat{y}_{2,j_2}$.

MULTI-AREA LEVEL i: Using the value $\tilde{y}_{i-1,j_{i-1}}$ provided by Level $i-1$ as measurements in a distributed approach, we can estimates the $y, \tilde{i}, j_i$ as

$$\left[F_{i,j_{i-1}}^T G_{i-1,j_{i-1}} F_{i,j_{i-1}})\right] \Delta\tilde{y}_{i-1,j_{i-1}}(k) = \\ F_{i,j_{i-1}}^T G_{i-1,j_{i-1}} \left[\tilde{y}_{i-1,j_{i-1}} - f_{i,j_{i-1}}(y_i(k))\right] \tag{28}$$

$$\left[F_{i,b_i}^T G_{i-1,b_{i-1}} F_{i,b_i}\right] \Delta\tilde{y}_{i-1}(k) = \\ F_i^T G_{i-1,b_{i-1}} \left[\tilde{y}_{i-1} - f_i(y_i(k))\right] \tag{29}$$

The Jacobian matrices are updated based on the estimation values obtained at level i, and also due to the estimation values at level $i+1$.

LEVEL l: Using the value $\tilde{y}_{l_1}$ provided by the lower level $l-1$, in a multi-area context as "measurement" vector, state estimation obtains the estimate $\hat{y}_l$ by iteratively solving the resulting normal equations

$$\left[F^T_{l,j_{l-1}} G_{l-1,j_{l-1}} F_{l,j_{l-1}})\right] \Delta\tilde{y}_{l-1,j_{l-1}}(k) =$$
$$F^T_{l,j_{l-1}} G_{l-1,j_{l-1}} \left[\tilde{y}_{l-1,j_{l-1}} - f_{l,j_{l-1}}(y_l(k))\right] \quad (30)$$
$$\left[F^T_{l,b_l} G_{l-1,b_{l-1}} F_{l,b_l}\right] \Delta\tilde{y}_{l-1}(k) =$$
$$F^T_l G_{l-1,b_{l-1}} \left[\tilde{y}_{l-1} - f_l(y_l(k))\right] \quad (31)$$

where the "weighting" matrix is the gain matrix of level $l-1$ for internal measurements

$$G_{l-1,j_{l-1}} = F^T_{l-1,j_{l-1}} G^{-1}_{l-2,j_{l-2}} F_{l-1,j_{l-1}},$$

and

$$G_{l-1,b_{l-1}} = F^T_{l-1,b_{l-1}} G^{-1}_{l-2,b_{l-2}} F_{l-1,b_{l-1}}$$

is the gain matrix of level $l-1$ for the boundary measurements, obtained as juxtaposition of the sub-matrices obtained at level $l-1$. We also remark that $G_{0,j_0} = R_{1,j_1}$ and $G_{0,j_0,b_0} = R_{1,j_1,b_1}$.

6.3.2 *Two-Level Multi-Area Hierarchical State Estimator Formulation*

Considering the most straightforward configuration of a hierarchical systems where we omit the intervening layers, we obtain the base case also described e.g. in[44]. We observe that at level 1 (the leaf nodes of our tree graph), a power system can be partitioned into r non-overlapping areas S_j having n_j buses each and connected by tie-lines.

Each area is updated by a local WLS-based state estimator which is connected, by means of communication links, to a higher state estimator, represented at level 2 (l), as described in [44]. The three sequential problems, which express the measurement approach described in [44], can be extended to the multi-area formulation in the following way:

$$y_{0j} = f_{1j}(y_{1j}) + e_{1j}, \qquad j = 1, \ldots, r \quad (32)$$
$$y_{0b} = f_{1b}(y_1) + e_{1b} \quad (33)$$
$$y_1 = f_2(y_2) + e_2 \quad (34)$$

where

y_{0j} : $p_{0j} \times 1$ vector of internal or local measurements in area S_j at level 1;

y_{0b} : $p_b \times 1$ vector of boundary measurements at level 1;

y_{1j} : $p_{1j} \times 1$ vector of internal state vector in area S_j at level 1;

y_1 : $p_1 \times 1$ vector of system-wide state vector at level 1, where $p_1 = \sum_{j=1}^{r} p_{1j}$;

y_2 : $p_2 \times 1$ vector of state vector at level 2;

$f_{1j}(\cdot)$, $f_{1b}(\cdot)$, $f_2(\cdot)$: non-linear vector functions;

e_{1j}, e_{1b}, e_2 : Gaussian random error vectors.

As we are employing a weighted least squares algorithm, the multi-level and multi-area state estimation problem can be solved with the same sparse WLS minimisation mechanism:

$$J(y_2) = \sum_{j=1}^{r} \left[y_{0j} - f_{1j}(f_2(y_2))\right]^T R_{1j}^{-1} \left[y_{0j} - f_{1j}(f_2(y_2))\right] + \\ + \left[y_{0b} - f_{1b}(f_2(y_2))\right]^T R_{1b}^{-1} \left[y_{0b} - f_{1b}(f_2(y_2))\right] \quad (35)$$

where $R_{1j} = \text{cov}(e_{1j}) = \mathbb{E}(e_{1j}e_{1j}^T) = \text{diag}\left(\sigma_{11}^2 \cdots \sigma_{1m_{1j}}^2\right)$ and $R_{1b} = \text{cov}(e_{1b}) = \mathbb{E}(e_{1b}e_{1b}^T) = \text{diag}\left(\sigma_{11}^2 \cdots \sigma_{1m_{1b}}^2\right)$.

The estimated state $\hat{y_2}$ is the solution of the Equation 35, which satisfy the optimality condition $\frac{\partial J(y_2)}{\partial y_2}$, and that can be rewritten as follows:

$$\sum_{j=1}^{r} F_2^T F_{1j}^T R_{1j}^{-1} \left[y_{0j} - f_{1j}(f_2(\hat{y}_2))\right] + \\ F_2^T F_{1b}^T R_{1b}^{-1} \left[y_{0b} - f_{1b}(f_2(\hat{y}_2))\right] = 0 \quad (36)$$

where $F_{1j} = F_{1j}(y_{1j}) = \dfrac{\partial f_{1j}(y_{1j})}{\partial y_{1j}}, j = 1, \ldots, r$ is the Jacobian matrix ($p_{0j} \times p_{1j}$) of the function $f_{1j}, j = 1, \ldots, r$ and $F_{1b} = F_{1b}(y) = \dfrac{\partial f_{1b}(y_1)}{\partial y_1}$ is the Jacobian matrix ($p_{0b} \times p_1$) of the non-linear function f_{1b}, associated to the boundary measurements, which may be partitioned as follows:

$$F_{1b}(y_1) = \left[F_{11b}(y_{11}) \cdots F_{1rb}(y_{1r})\right] \quad (37)$$

This can then be rewritten as:

$$\sum_{j=1}^{r} F_{2j}^T F_{1j}^T R_{1j}^{-1} \left[y_{0j} - f_{1j}(f_{2j}(\hat{y}_2))\right] + \\ F_2^T F_{1b}^T R_{1b}^{-1} \left[y_{0b} - f_{1b}(f_2(\hat{y}_2))\right] = 0 \quad (38)$$

and, after some algebraical manipulations and also a linearisation of the terms $\hat{y_{1j}}$ and $\hat{y_1}$, we obtain:

$$\sum_{j=1}^{r} F_{2j}^T F_{1j}^T R_{1j}^{-1} \left[z_{1j} - + f_{1j}(\tilde{y}_{1j}) \right] +$$
$$+ \sum_{j=1}^{r} F_{2j}^T (F_{1j}^T R_{1j}^{-1} F_{1j}) \left[\tilde{y}_{1j} - f_{2j}(\hat{y}_2) \right] +$$
$$+ F_2^T F_{1b}^T R_{1b}^{-1} \left[z_{1b} - f_{1b}(\tilde{y}_1) \right] +$$
$$+ F_2^T (F_{1b}^T R_{1b}^{-1} F_{1b}) \left[\tilde{y}_1 - f_2(\hat{y}_2) \right] = 0 \tag{39}$$

At level 1, the boundary measurements can be decoupled following the areas as $z_{1jb} = f_{1jb}(\tilde{y}_{1j})$, in order to obtain:

$$\sum_{j=1}^{r} F_{2j}^T F_{1j}^T R_{1j}^{-1} \left[y_{0j} - f_{1j}(\tilde{y}_{1j}) \right] +$$
$$+ \sum_{j=1}^{r} F_{2j}^T (F_{1j}^T R_{1j}^{-1} F_{1j}) \left[\tilde{y}_{1j} - f_{2j}(\hat{y}_2) \right] +$$
$$+ \sum_{j=1}^{r} F_{2j}^T F_{1jb}^T R_{1jb}^{-1} \left[y_{0jb} - f_{1jb}(\tilde{y}_{1j}) \right] +$$
$$+ F_2^T (F_{1b}^T R_{1b}^{-1} F_{1b}) \left[\tilde{y}_1 - f_2(\hat{y}_2) \right] = 0 \tag{40}$$

where R_{1jb} is the diagonal covariance sub-matrix of R_{1jb}, whose elements are connected to area S_j. It is important to note that the Jacobian matrices F_{1j}, F_{1jb}, and F_2 should be computed at the solution point $([\tilde{y}_{11}, \ldots, \tilde{y}_{1r}], \hat{y}_2)$, with $\tilde{y}_1 = f_2(\hat{y}_2)$.

The solution to the original problem (36) can then be decomposed into two successive levels, each involving the solution of a WLS problem, which can be summarised as follows:

1. *Multi-Area Level 1*. Obtain the estimate $\tilde{y}_{1j}$ for each area S_j by iteratively solving the associated normal equations

$$\left[F_{1j}^T R_{1j}^{-1} F_{1j} \right] \Delta\tilde{y}_{1j}(k) = F_{1j}^T R_{1j}^{-1} \left[y_{0j} - f_{1j}(y_{1j}(k)) \right] \tag{41}$$
$$\left[F_{1jb}^T R_{1jb}^{-1} F_{1jb} \right] \Delta\tilde{y}_{1j}(k) = F_{1jb}^T R_{1jb}^{-1} \left[y_{0jb} - f_{1jb}(y_{1j}(k)) \right] \tag{42}$$

   The inputs at this level are the measurement vector y_{0j} and y_{0jb} and the matrices F_{1j}, F_{1jb}, R_{1j} and R_{1jb}. The Jacobians F_{1j} and F_{1jb} are updated at each iteration, according to the current value $y_{1j}(k)$ and $y_{1jb}(k)$. These Jacobians F_{1j} and F_{1jb} must also be recomputed every time the higher level (here: level 2) produces a new value for $\hat{y}_2$. The matrices F_{1j}, F_{1jb} depend on the vector $\hat{y}_1 = f_2(\hat{y}_2)$.

2. *Multi-Area Level 2*. Using the value $\tilde{y}_1$ provided by multi-area level 1 as the "measurement" vector, our state estimation obtains the estimate $\hat{y}_2$ by iteratively solving the resulting normal equations

$$\left[F_{2j}^T G_{1j} F_{2j})\right] \Delta\tilde{y}_{1j}(k) = F_{2j}^T G_{1j} \left[\tilde{y}_{1j} - f_{2j}(y_2(k))\right] \tag{43}$$

$$\left[F_{2b}^T G_{1b} F_{2b}\right] \Delta\tilde{y}_1(k) = F_2^T G_{1b} \left[\tilde{y}_1 - f_2(y_2(k))\right] \tag{44}$$

where the weighting matrix

$$G_{1j} = F_{1j}^T R_{1j}^{-1} F_{1j}$$

is the gain matrix of level 1 for internal measurements, and $G_{1b} = F_{1b}^T R_{1b}^{-1} F_{1b}$ the gain matrix of level 1 for the boundary measurements, obtained as juxtaposition due to equation (37). Then, computation of level 2 should be repeated with updated values of $\tilde{y}_{1j}$, until level 2 provides values satisfying tolerance constraints for $\hat{y}_2$ in two consecutive runs.

6.3.3 *A Two-Level Instance of the Multi-Area Hierarchical State Estimator*

Power state estimation refers to the procedure of obtaining voltage and angle estimated values at all the system buses at a given point in time. As described in [5] the power system is conventionally modelled — even for a 3-phase system — as the single phase positive sequence circuit for modeling the entire system. Transmission lines are represented by *two-port* networks π whose parameters corresponding to the positive sequence equivalent circuit of transmission lines. [5]. A general scheme of the equivalent circuit is shown in figure 34 below.

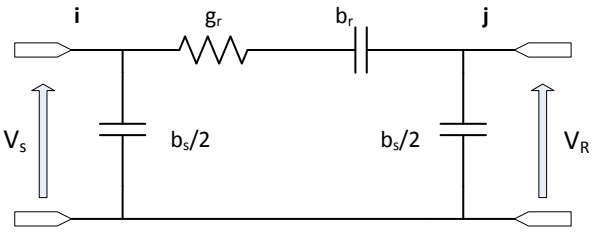

Figure 34: Transmission Line Equivalent Circuit: Medium/Long-Length Line

The solution adopted and implicitly accepted as standard in all WLS implementation is one using the shunt impedance representation also known as *medium length*. This equivalent circuit fits quite well, without introducing relevant approximation mistakes, for transmission lines with lengths on the order of 80–250km. As our research is primarily oriented towards micro-grid scenarios, we consider the

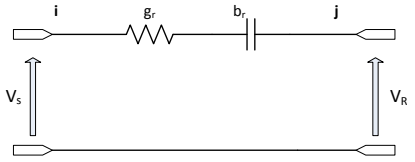

Figure 35: Transmission Line Equivalent Circuit: Short Length Line

short line approximation representation as a viable approximation for our reference model and validation system. The short length equivalent 2-port model can be used for representing transmission lines no longer than 80km; this limitation is due to shunt impedance simplification. The centralised state estimation algorithm as detailed in [5] is usually represented by using as state variables the voltage magnitude V_k at the bus k, active/reactive power branch flow between two branches, e.g k and m, active/reactive power bus injection into the bus k, and — in addiction to those state variables — the model proposed uses the current magnitude measurements.

The choice of adopting the WLS state estimation with the addition of the current measurements found its motivation in the consideration of the future operational contexts in which, besides having a greater availability of data sets, it will be ever more to integrate local power production (e.g. photovoltaic panels, wind-farm, batteries, and other generators) simultaneously, one would also find generators removed as e.g. electric vehicles or hybrid vehicles may change location or become inactive.

The state variable data sets described by [5], applied to this imminent and not even too ambitious scenario, would not satisfy these demands for the following reasons:

- The distribution infrastructures will be subject to a migration from the static approach to a dynamic one on which the interconnections will change according to variable needs (e.g. electric mobility)
- There will be some electrical devices for which the intrinsic electrical parameters (load resistance/reactance, charging times, etc.) may not be fully known or trusted except for their absorption of electric current.

In those circumstances, the model presented here is a conservative WLS-based state estimator modified with the addition of the current measurement. These changes have an impact on the structure of the matrix H, which represent the Jacobian, used to estimate the solution

of the problem WLS. The resulting matrix H of the Jacobian is then given in equation (45):

$$\mathbf{H1} = \begin{bmatrix} \widehat{P_{inj}} \\ \widehat{P_{flow}} \\ I_{measurement} \\ V_{measurement} \end{bmatrix} = \begin{bmatrix} \frac{\partial P_{inj}}{\partial \theta} & \frac{\partial P_{inj}}{\partial V} \\ \frac{\partial P_{flow}}{\partial \theta} & \frac{\partial P_{flow}}{\partial V} \\ \frac{\partial Q_{inj}}{\partial \theta} & \frac{\partial Q_{inj}}{\partial V} \\ \frac{\partial Q_{flow}}{\partial \theta} & \frac{\partial Q_{flow}}{\partial V} \\ \frac{\partial \theta_{V,measured}}{\partial \theta} & \frac{\partial \theta_{V,measured}}{\partial V} \\ \frac{\partial V_{measured}}{\partial \theta} & \frac{\partial V_{measured}}{\partial V} \\ \frac{\partial \theta_{I,measured}}{\partial \theta} & \frac{\partial \theta_{I,measured}}{\partial V} \\ \frac{\partial I_{measured}}{\partial \theta} & \frac{\partial I_{measured}}{\partial V} \end{bmatrix} \tag{45}$$

By applying the scheme described in Figure 35 it is now possible to obtain the formulation of the current that flows from across the equivalent line impedance:

$$\widehat{I_{ij}} = \frac{\widehat{V_s} - \widehat{V_R}}{g_{ij} + jb_{ij}} \tag{46}$$

where $\widehat{I_{ij}}$ is the current phasor expressed accordingly in rectangular form:

$$\widehat{I_{ij}} = I_{ij}\left[\cos\delta_{ij} + j\sin\delta_{ij}\right] \tag{47}$$

By applying the Kirchhoff nodal and mesh laws, the branch current is determined as:

$$\widehat{I_{ij}} = \frac{\widehat{V_s} - \widehat{V_R}}{g_{ij} + jb_{ij}} \tag{48}$$

where $\widehat{V_s}$ and V_R are respectively the phase of the measured voltage at the port **1** and the port **2**:

$$\widehat{V_s} = V_s\left(\cos\delta_s + j\sin\delta_s\right)$$
$$\widehat{V_R} = V_R\left(\cos\delta_R + j\sin\delta_R\right)$$

$\widehat{V_s}$, $\widehat{V_R}$ and $\widehat{I_{ij}}$ are represented as

$$\widehat{I_{ij}} = \frac{V_s\cos\delta_s + jV_s\sin\delta_s + V_R\cos\delta_R + jV_R\sin\delta_R}{g_{ij}^2 + jb_{ij}^2} \tag{49}$$

Expressing I_{ij} according to the rectangular representation, it is possible to separate the real part from the imaginary:

$$\widehat{I_{ij}} = C + jD \tag{50}$$

$$C = \frac{V_s \left[g_{ij}\cos\delta_s + b_{ik}\sin\delta_s\right] - V_R \left[g_{ij}\cos\delta_R + b_{ij}\sin\delta_R\right]}{g_{ij}^2 + b_{ij}^2} \tag{51}$$

$$D = \frac{-V_s \left[b_{ij}\cos\delta_s - g_{ij}\sin\delta_s\right] + V_R \left[b_{ij}\cos\delta_R - g_{ij}\sin\delta_R\right]}{g_{ij}^2 + b_{ij}^2} \tag{52}$$

The parameters to be estimated are now the following:

$$I_{ij} = \left[C^2 + D^2\right]^{\frac{1}{2}} \tag{53}$$

$$\theta_{ij} = \tan^{-1}\left(\frac{D}{C}\right) \tag{54}$$

We now have the power flow equations

$$P_{ij} + jQ_{ij} = \widehat{V_{ij}}\,\widehat{I_{ij}}^{*} \tag{55}$$

where the $\widehat{V_{ij}}$ and $\widehat{I_{ij}}^{*}$ represent the complex values of the voltage and the current written in rectangular coordinates:

$$\widehat{I_{ij}} = I_{ij}\cos\theta + j\cos\theta \tag{56}$$

$$\widehat{V_s} = V_s\cos\alpha + j\cos\alpha \tag{57}$$

$$\begin{aligned} P_{ij} + Q_{ij} &= VsI_{ij}\left(\cos\delta_s + j\sin\delta_s\right)\left(\cos\theta + j\sin\theta\right) \\ &= VsI_{ij}\left[\cos\left(\alpha-\theta\right) + j\sin\left(\alpha-\theta\right)\right] \end{aligned} \tag{58}$$

The partial derivatives of the of θ_{ij} and I_{ij} needed to construct the sub-matrices of $\frac{\partial\theta_{I,measured}}{\partial\theta}$, $\frac{\partial\theta_{I,measured}}{\partial V}$, $\frac{\partial I_{measured}}{\partial\theta}$ and $\frac{\partial I_{measured}}{\partial V}$ can be obtained by using the following simplified representations:

$$\dot{\theta} = \frac{C\dot{D} - D\dot{C}}{C^2 + D^2} \tag{59}$$

$$\dot{I_{ij}} = \frac{C\dot{C} + D\dot{D}}{\sqrt{SC^2 + D^2}} \tag{60}$$

6.3.4 *Performance Metrics and Results*

We have evaluated the performance of the proposed hierarchical model in terms of the following performance metrics:

1. **Estimation accuracy:**

   We chose the the bus phase angle and voltage magnitude difference between hierarchical and centralised algorithms as the performance metrics for evaluating the convergence of our proposed algorithms:

$$\theta_{j,k}(i) = \theta_{j,k}^{(h)} - \theta_{j,k}^{(c)} \tag{61}$$

   where subscripts j and k correspond to buses j and k, respectively. The terms $\theta_{j,k}^{(h)}$ and $\theta_{j,k}^{(c)}$ represent the absolute values of bus j and k's phase angle differences in both the state estimation models. Correspondingly, the voltage metric is:

$$E_j = \hat{V}_j^{(h)} - \hat{V}_j^{(c)} \tag{62}$$

   where $\hat{V}_j^{(h)}$ and $\hat{V}_j^{(c)}$ represent bus j's estimated voltage magnitude in hierarchical and centralised variants, respectively.

2. **Execution time efficiency:** Another important metric is the execution time efficiency of the our proposed algorithms, which can be evaluated as:

$$\textit{Efficiency}(\%) = \frac{T_c}{T_h} * 100 \tag{63}$$

   where T_c and T_h are the system execution time of both state estimation algorithms.

6.3.4.1 *Numerical Validation*

In this section we want to present some results of simulations performed using our state estimator model realised using Matlab. The network used for these trials is the well-known IEEE 118 bus test network (obtained from [56]), which has been divided into 8 sub-areas, as can be seen in figure 36.

The specific 118 bus data used in this simulation are taken from [93] All simulations have been preformed on a commodity laptop (Intel I7-2630Q, 8GB RAM). The benchmark metrics described above in section 6.3.4 have been used for evaluating the model proposed in

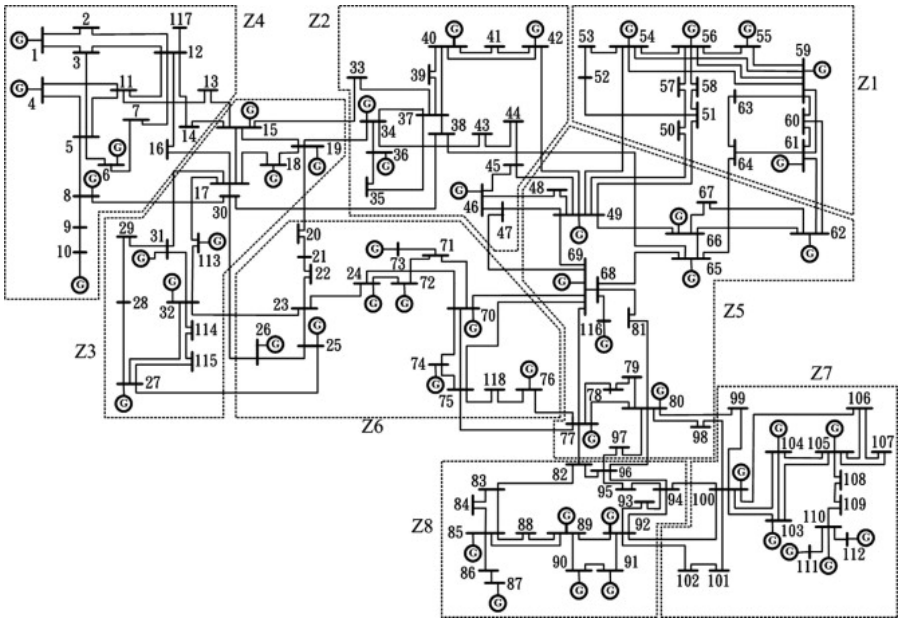

Figure 36: IEEE 118 Bus Test Network: Sub-Division Areas Schema

Measurement	Factorisation	Mean	Cov.
Phase	YES	-2.2925	44.19
Voltage	YES	-0.0380	0.0051
Phase	NO	-2.7372	24.2611
Voltage	NO	-0.0394	0.0051

Table 11: Aggregate Estimation Accuracy Values

this chapter both for the case of matrix factorisation and with factorisation omitted. For the estimation accuracy we obtain the aggregate values shown in table 11:

This gives us an execution time efficiency coefficient of 122% for the model without the factorisation, and 226.7% in the case including factorisation relative to the simple centralised model, respectively.

6.4 STATE ESTIMATOR ROBUSTNESS

The iterative solution of the WLS problem described in 17 requires the evaluation of the inverse of the matrix G and other square matrices, such as one that expresses the covariance of the error measurement (R_I) parameter which is related to the measurement instrumentation used to perform voltage, current, and power detection for each bus bar.

Even when employing the extended forms of the normal equation for the hierarchical models both in the multi-area formulation (see equations 35, 22, 44) susceptible to such inversion operations. For real systems that are not idealised such as the models based on op-

timal power flow, *in particular those where a particular partitioning of the state estimator is externally forced*, this requires the consideration of *numerical stability*.

6.4.1 *Conditioning and Stability of State Estimator Operation*

The condition number of a square matrix A is defined [43] as the product of the norm of A and the norm of A^{-1}:

$$cond[A] = \|A\| \left\|A^{-1}\right\| \tag{64}$$

The condition number of a matrix provides an estimate of how much the uncertainty in the right hand side of $A\underline{x} = b$ may be magnified in the solution of:

$$\|\delta\underline{x}\| \ \|\underline{x}\| = cond(A) \, \|\delta b\| \, \|b\| \tag{65}$$

In all the WLS realisations of state estimators mentioned in chapter 6.2, we have noted that none have imposed any criteria for the conditioning of the gain matrix G, which is a major source of numerical instability. However, particularly for power systems that are rapidly changing as is likely to be the case in smart grids and also for the distributed (hierarchical) models considered here, it is strictly necessary to control for stability.

This is a general property of any forward-backwards substitution equation solving method found in WLS state estimation algorithms, as these rely on matrix inversion where parameters will differ by several orders of magnitude. We also note that this is a particular issue arising in the error measurement error covariance matrix obtained from the measurements data set exchanged through the data channel used by the state estimation system *which may hence be the subject of manipulation by an adversary*.

We observe that such manipulations are not captured by any of the bad data injection detection approaches identified in section 6.2 as stability problems will affect a large number of parameters.

Where ill-conditioned matrices cannot be avoided as is the case here, a number of numerical approaches can be considered which may be applied to the normal equations (eq. 65) to minimise the stability problem. A common approach is the LU factorisation in conjunction Peters-Wilkinson method (see [47] and the orthogonal factorisation QR [60, 98, 28]).

However, any such factorisation method inherently sacrifices the precision of the matrix (in particular matrix G in equation 14) and therefore reduces the ability to detect malicious manipulation.

6.4.2 *Error Covariance Matrix Manipulation Attack*

We note that the problem described in the preceding section does not arise in simplified models using a linearised (DC) approach, which related work on malicious bad data injection, but also distributed state estimation models such as that of Xie *et al.*[101] rely on.

Whenever such a network cannot be assumed a priori to avoid ill-conditioned matrices or indeed attacks injecting such inter-relations among parameters *rather than individual bad measurements*, it will be possible to force the WLS to desired values, and to arbitrarily increase the number of iterations required up to non-convergence whilst increasing the error of the state estimator.

The fact that this stability is partly related to the network topology has led us to the discovery that state estimators are vulnerable to manipulations of the bus-bar interconnections which future smart grid systems are likely to change more frequently than conventional grids. Similarly, we note that any errors (malicious or otherwise) in estimated parameters will affect the entire state estimator hierarchy unless explicit counter-measures are in place. Existing hierarchical and distributed state estimators do not appear to make provisions for cases where one or more sub-areas or partitions do not converge and will hence force the overall system into an unstable or non-convergent state. This also holds true for approaches relying on an explicit "anchor" sub-area (e.g. in the trusted areas method of Pajic and Clements [71]), and introduces a higher *resilience threshold*.

6.4.3 *State Estimator Parameter Criteria*

Clearly, not all parameters identified in the preceding section have equal influence on the validity of the state estimate. It is therefore important to consider which parameters are exchanged by the WLS state estimation (these are used for local state estimation) and which may hence be targeted by attackers, namely:

- Bus-bar voltage and phase
- Branches connecting network bus-bars
- Error measurement covariance
- Branch impedance
- Branch susceptance
- Load susceptance (where this is not neglected)

Not all parameters will be transmitted, and some may be either assumed as known to all state estimators or as pre-determined. A similar analysis not presently considered in related work is required

for the number of iterations (or bounds, respectively) for the WLS algorithm to converge. In extreme cases this will result in failure to reach convergence.

6.5 CONCLUSIONS

The State Estimation problem in Smart Grids is presented with a hierarchical structure. Some analyses has been performed and presented in this Chapter. The convergence analysis is an on-going problem.

Further enhancements are related to possible data injection problems. The hierarchical and centralized models can be compared respect the robustness to data injection attacks.

7

CONCLUSIONS AND FUTURE WORKS

Industrial control system (ICS) includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. ICS are typically used in industries such as electrical, water and waste-water, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing. These control systems are critical to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems.

In this thesis some possible enhancement are discussed in order to increase the awareness of operator with information coming from other infrastructures or from national and international agencies. The author main works are related to the on-line trouble of modelling techniques in distributed context. In fact, the validation and test phases are a very important moment, approaching real infrastructures and all the problem related to time constraints.

The study of Data Fusion techniques, and especially Evidence Theory framework, enriches the Critical Infrastructure models with the possibility to merge data and information. In this case, the analysis is just a mathematical work with some sketching example in real-time context. The main enhancement is related to the possible application in the Critical Infrastructure Protection. The main drawback is still related to time constraints. In fact, Evidence Theory needs a very small set of hypotheses in order to deal with real-time analysis.

The presented work is still ongoing, and possible enhancements include the study of heuristics for the Evidence Theory and the evaluation of the power set. Other results can be obtained regarding the evolution of the knowledge models in order to represents also other and new possibility.

Smart Grids area electricity networks that can efficiently integrate the behaviour and actions of all users connected to it, in order to guar-

antee an economic efficient and sustainable power system. A possibility is to change the state estimation in order to consider also hierarchical structure with different vendor and islands.

The improvements in power state estimation are many and they are related to the amount of information exchanged among levels. This information flow also generate trouble from the security point of view, with new vectors for cyber attacks.

BIBLIOGRAPHY

[1] Fp7 micie project, 2010. http://www.micie.eu.

[2] http://dictionary.reference.com, 2011.

[3] Fp7 cockpitci project, 2012. http://www.cockpitci.eu.

[4] Snort, 2012. http://www.snort.org.

[5] Ali Abur and Antonio Gómez Expósito. *Power System State Estimation: Theory and Implementation*. CRC Press, Boca Raton, FL, USA, 2004.

[6] Carlisle Adams, Stephen Farrell, Tomi Kause, and Tero Mononen. Internet x. 509 public key infrastructure certificate management protocol (cmp). *Request for Comments (RFC)*, 4210, 2005.

[7] Saurabh Amin, Galina Schwartz, and S Sastry. Security interdependencies for networked control systems with identical agents. *Decision and Game Theory for Security*, pages 107–122, 2010.

[8] Paul Barford, Marc Dacier, Thomas G Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, et al. Cyber sa: Situational awareness for cyber defense. *Cyber Situational Awareness*, 46:3–13, 2010.

[9] Dimitri P. Bertsekas and John N. Tsitsiklis. *Parallel and Distributed Computation: Numerical Methods*. Prentice-Hall, Englewood Cliffs, 1989.

[10] James C Bezdek and Sanker K Pal. *Fuzzy models for pattern recognition*, volume 23. IEEE press New York, 1992.

[11] Erik Blasch and Susan Plano. Dfig level 5 (user refinement) issues supporting situational assessment reasoning. In *Information Fusion, 2005 8th International Conference on*, volume 1, pages xxxv–xliii. IEEE, 2005.

[12] John R Boyd. A discourse on winning and losing. 1987.

[13] Stephen Boyd, Arpita Ghosh, Balaji Prabhakar, and Devavrat Shah. Randomized gossip algorithms. *Information Theory, IEEE Transactions on*, 52(6):2508–2530, 2006.

[14] Benjamin A Carreras, David E Newman, Paul Gradney, Vickie E Lynch, and Ian Dobson. Interdependent risk in interacting infrastructure systems. In *System Sciences, 2007. HICSS 2007. 40th*

Annual Hawaii International Conference on, pages 112–112. IEEE, 2007.

[15] Rui Chang, Wilfried Brauer, and Martin Stetter. 2008 special issue: Modeling semantics of inconsistent qualitative knowledge for quantitative bayesian network inference. *Neural Networks*, 21(2-3):182–192, 2008.

[16] Shuguang Cui, Zhu Han, Soummya Kar, Tung T. Kim, H. Vincent Poor, and Ali Tajer. Coordinated Data-Injection Attack and Detection in the Smart Grid: A detailed look at enriching detection solutions. *IEEE Signal Processing Magazine*, 29(5):106–115, September 2012. doi: 10.1109/MSP.2012.2185911.

[17] Yogen K. Dalal. A distributed algorithm for constructing minimal spanning trees. *Software Engineering, IEEE Transactions on*, SE-13(3):398–405, 1987.

[18] Thyagaraju Damarla. Hidden markov model as a framework for situational awareness. In *Information Fusion, 2008 11th International Conference on*, pages 1–7. IEEE, 2008.

[19] Subrata Kumar Das. *High-level data fusion*. Artech House Publishers, Norwood, MA, USA, 2008.

[20] Stefano De Porcellinis, Roberto Setola, Stefano Panzieri, and Giovanni Ulivi. Simulation of heterogeneous and interdependent critical infrastructures. *International Journal of Critical Infrastructures*, 4(1):110–128, 2008.

[21] Stefano De Porcellinis, Stefano Panzieri, and Roberto Setola. Modelling critical infrastructure via a mixed holistic reductionistic approach. *International Journal of Critical Infrastructures*, 5 (1):86–99, 2009.

[22] Arthur Dempster. Upper and lower probabilities induced by a multivalued mapping. *Classic Works of the Dempster-Shafer Theory of Belief Functions*, 219:57–72, 2008.

[23] Ethan Dereszynski, Jesse Hostetler, Alan Fern, Tom Dietterich, Thao-Trang Hoang, and Mark Udarbe. Learning probabilistic behavior models in real-time strategy games. In *Seventh Artificial Intelligence and Interactive Digital Entertainment Conference*, 2011.

[24] C Di Mauro, S Bouchon, C Logtmeijer, RD Pride, T Hartung, and JP Nordvik. A structured approach to identifying european critical infrastructures. *International Journal of Critical Infrastructures*, 6(3):277–292, 2010.

[25] G. Digioia, C. Foglietta, G. Oliva, S. Panzieri, and R. Setola. Moving from looking to understanding: Situation awareness and prediction. In *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*. CRC Press / Taylor & Francis eds., To Appear.

[26] Giusj Digioia, Chiara Foglietta, Gabriele Oliva, and Stefano Panzieri. Aware online interdependency modelling via evidence theory. *International Journal of Critical Infrastructures*, 9 (1):74–92, 2013.

[27] Naganand Doraswamy and Dan Harkins. *IPSec: the new security standard for the Internet, intranets, and virtual private networks*. Prentice Hall, 2003.

[28] Zhengchun Du, Zhenyong Niu, and Wanliang Fang. Block QR Decomposition Based Power System State Estimation Algorithm. *Electric Power Systems Research*, 76(1–3):86–92, September 2005. doi: 10.1016/j.epsr.2005.04.004.

[29] Didier Dubois and Henri Prade. Possibility theory as a basis for qualitative decision theory. In *International Joint Conference on Artificial Intelligence*, volume 14, pages 1924–1932. Lawrence Erlaum Associates LTD, 1995.

[30] Leonardo Dueñas-Osorio, James I Craig, Barry J Goodno, and Ann Bostrom. Interdependent response of networked systems. *Journal of Infrastructure Systems*, 13(3):185–194, 2007.

[31] Mica R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1):32–64, 1995.

[32] M.R. Endsley. Design and evaluation for situation awareness enhancement. *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 32(2):97–101, 1988.

[33] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. Technical report, White paper, Symantec Corp., Security Response, 2011.

[34] Laurene V. Fausett. *Fundamentals of neural networks: architectures, algorithms, and applications*. Prentice-Hall Englewood Cliffs, NJ, 1994.

[35] John D Fernandez and Andres E. Fernandez. Scada systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, 20(4):160–168, 2005.

[36] Flavio Fiorini, Andrea Gasparri, Maurizio Di Rocco, and Giovanni Ulivi. Distributed data aggregation via networked transferable belief model over a graph. In *Robotics and Automation (ICRA), 2011 IEEE International Conference on*, pages 5730–5736. IEEE, 2011.

[37] Francesco Flammini, Valeria Vittorini, Nicola Mazzocca, and Concetta Pragliola. A study on multiformalism modeling of critical infrastructures. *Critical Information Infrastructure Security*, pages 336–343, 2009.

[38] Scott E Friedman and Kenneth D Forbus. Repairing incorrect knowledge with model formulation and metareasoning. In *Proceedings of the Twenty-Second international Joint Conference on Artificial Intelligence*, volume 22, pages 887–893. AAAI Press, 2011.

[39] Andrea Gasparri, Gabriele Oliva, and Stefano Panzieri. On the distributed synchronization of on-line iim interdependency models. In *Proceedings of the 7th IEEE International Conference on Industrial Informatics*, pages 795–800. IEEE, June 2009.

[40] Andrea Gasparri, Flavio Fiorini, Maurizio Di Rocco, and Stefano 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, 2012.

[41] James Geller, Huanying Gu, Yehoshua Perl, and Michael Halper. Semantic refinement and error correction in large terminological knowledge bases. *Data & Knowledge Engineering*, 45(1):1–32, 2003.

[42] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart Grid Data Integrity Attacks: Characterisations and Countermeasures. In *Proceedings of the 2011 Second IEEE International Conference on Smart Grid Communications (SmartGridComm 2011)*, pages 232–237, Brussels, Belgium, October 2011. IEEE Press. doi: 10.1109/SmartGridComm.2011.6102324.

[43] G.H. Golub and C.F. Van Loan. Matrix computations. 1996. *Johns Hopkins University, Press, Baltimore, MD, USA*, 1996.

[44] Antonio Gómez Expósito, Ali Abur, Antonio de la Villa Jaén, and Catalina Gómez-Quiles. A Multilevel State Estimation Paradigm for Smart Grids. *Proceedings of the IEEE*, 99(6):952–976, June 2011. doi: 10.1109/JPROC.2011.2107490.

[45] Antonio Gómez Expósito, Antonio de la Villa Jaén, Catalina Gómez-Quiles, Patricia Rousseaux, and Thierry van Cutsem. A Taxonomy of Multi-Area State Estimation Methods. *Electric Power Systems Research*, 81(4):1060–1069, April 2011. doi: 10.1016/j.epsr.2010.11.012.

[46] Chloe Griot. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation. *International Journal of Critical Infrastructures*, 6(4):363–379, 2010.

[47] J.W. Gu, K.A. Clements, G.R. Krumpholz, and P.W. Davis. The solution of ill-conditioned power system state estimation problems via the method of peters and wilkinson. *Power Apparatus and Systems, IEEE Transactions on*, PAS-102(10):3473 –3480, oct. 1983. ISSN 0018-9510. doi: 10.1109/TPAS.1983.317846.

[48] Yacov Y Haimes and Pu Jiang. Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure systems*, 7(1):1–12, 2001.

[49] Jim W Hall and Jonathan Lawry. Generation, combination and extension of random set approximations to coherent lower and upper probabilities. *Reliability Engineering & System Safety*, 85 (1):89–101, 2004.

[50] H. Jeong, S. P. Mason, A. L. Barabasi, and Z. N. Oltvai. Lethality and centrality in protein networks. *Nature*, 411(6833):41–42, 2001.

[51] G. N. Korres. A distributed multiarea state estimation. *IEEE Transactions on Power Systems*, 26(1):73–84, February 2011.

[52] Kosut, O. and Jia, L. and Thomas, R. J. and Tong, L. Malicious Data Attacks on the Smart Grid. *IEEE Transactions on Smart Grid*, 2(4):645–658, Dec. 2011. doi: doi:10.1109/TSG.2011.2163807.

[53] Maciej Kurant and Patrick Thiran. Layered complex networks. *Physical review letters*, 96(13):138701, 2006.

[54] Earl E Lee, John E Mitchell, and William 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, 2007.

[55] Martin E. Liggins, David L. Hall, and James Llinas. *Handbook of multisensor data fusion: theory and practice*, volume 22. CRC Press, 2008.

[56] S.-S. Lin. An efficient algorithm for state estimation problems with coupling inequality constraints. *Applied Mathematics and Computation*, pages 492 – 501, 2007. doi: 10.1016/j.amc.2007.04.051.

[57] Yao Liu, Peng Ning, and Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids. In Somesh Jha and Angelos D. Keromytis, editors, *Proceedings*

of the 16th ACM Conference on Computer and Communications Security, pages 21–32, Chicago, IL, USA, November 2009. ACM Press. doi: 10.1145/1653662.1653666.

[58] Andreas A. Malikopoulos, Panos Y. Papalambros, and Dennis N. Assanis. A real-time computational learning model for sequential decision-making problems under uncertainty. *Journal of Dynamic Systems, Measurement, and Control*, 131:041010.1–04101.8, 2009.

[59] A. Monticelli. Electric Power System State Estimation. *Proceedings of the IEEE*, 88(2):262–282, February 2000. doi: 10.1109/5.824004.

[60] A. Monticelli, C.A.F. Murari, and F.F. Wu. A hybrid state estimator: Solving normal equations by orthogonal transformations. *Power Apparatus and Systems, IEEE Transactions on*, PAS-104(12): 3460 –3468, dec. 1985. ISSN 0018-9510. doi: 10.1109/TPAS.1985.318896.

[61] DE Newman, Bertrand Nkei, BA Carreras, Ian Dobson, VE Lynch, and Paul Gradney. Risk assessment in complex interacting infrastructure systems. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, pages 63c–63c. IEEE, 2005.

[62] K-C Ng and Bruce Abramson. Uncertainty management in expert systems. *IEEE Expert: Intelligent Systems and Their Applications*, 5(2):29–48, 1990.

[63] Thomas Dyhre Nielsen and Finn Verner Jensen. *Bayesian networks and decision graphs*. Springer Publishing Company, Inc., 2007.

[64] AH Nieuwenhuijs, HAM Luiijf, and MHA Klaver. Modeling critical infrastructure dependencies. *IFIP International Federation for Information Processing, Critical Infrastructure Protection. E. Goetz, and S. Shenoi (eds.), Boston: Springer*, 2008.

[65] United States. Dept. of Homeland Security. *National Infrastructure Protection Plan*. DIANE Publishing, 2008.

[66] Reza Olfati-Saber and Richard M Murray. Consensus problems in networks of agents with switching topology and time-delays. *Automatic Control, IEEE Transactions on*, 49(9):1520–1533, 2004.

[67] Gabriele Oliva, Stefano Panzieri, and Roberto Setola. Agent-based input-output interdependency model. *International Journal of Critical Infrastructure Protection*, 3(2):76–82, 2010.

[68] Gabriele Oliva, Stefano Panzieri, and Roberto Setola. Fuzzy dynamic input-output inoperability model. *International Journal of Critical Infrastructure Protection*, 4(3-4):165–175, 2011.

[69] Gabriele Oliva, Stefano Panzieri, and Roberto Setola. Online distributed interdependency estimation for critical infrastructures. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pages 7224–7229. IEEE, 2011.

[70] Gabriele Oliva, Stefano Panzieri, and Roberto Setola. Distributed synchronization under uncertainty: a fuzzy approach. *Fuzzy Sets and Systems*, 206:103–120, 2012.

[71] S. Pajic and K. A. Clements. Power System State Estimation via Globally Convergent Methods. *IEEE Transactions on Power Systems*, 20(4):1683–1689, November 2005. doi: 10.1109/TPWRS.2005.857383.

[72] Stefano Panzieri and Roberto Setola. Failures propagation in critical interdependent infrastructures. *International Journal of Modelling, Identification and Control*, 3(1):69–78, 2008.

[73] Peter Pederson, D Dudenhoeffer, Steven Hartley, and May Permann. Critical infrastructure interdependency modeling: a survey of us and international research. *Idaho National Laboratory*, pages 1–20, 2006.

[74] Leonid Portnoy, Eleazar Eskin, and Sal Stolfo. Intrusion detection with unlabeled data using clustering. In *In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001*. Citeseer, 2001.

[75] Upeka Kanchana Premaratne, Jagath Samarabandu, Tarlochan S Sidhu, Robert Beresh, and Jian-Cheng Tan. An intrusion detection system for iec61850 automated substations. *Power Delivery, IEEE Transactions on*, 25(4):2376–2383, 2010.

[76] Craig G Rieger, David I Gertman, and Miles A McQueen. Resilient control systems: Next generation design research. In *Human System Interactions, 2009. HSI'09. 2nd Conference on*, pages 632–636. IEEE, 2009.

[77] Steven M Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on*, volume 2, pages 1–8. IEEE, 2004.

[78] Steven M Rinaldi, James P Peerenboom, and Terrence K Kelly. Identifying, understanding, and analyzing critical infrastruc-

ture interdependencies. *Control Systems, IEEE*, 21(6):11–25, 2001.

[79] Billy Rios and Terry McCorkle. 100 bugs in 100 days: an analysis of ics (scada) software. Technical report, Presented at Session DerbyCon, 2011.

[80] V Rosato, L Issacharoff, F Tiriticco, S Meloni, S Porcellinis, and R Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1):63–79, 2008.

[81] Y. Saad and Y. Saad. *Iterative methods for sparse linear systems*, volume 620. PWS publishing company Boston, 1996.

[82] Roberto Setola, Stefano De Porcellinis, and Marino Sforna. Critical infrastructure dependency assessment using the input–output inoperability model. *International Journal of Critical Infrastructure Protection*, 2(4):170–178, 2009.

[83] Glenn Shafer. *A mathematical theory of evidence*, volume 76. Princeton university press Princeton, 1976.

[84] Elisa Shahbazian, Dale E Blodgett, and Paul Labbé. The extended ooda model for data fusion systems. In *Proceedings of the 4th International Conference on Information Fusion, Fusion'2001*, 2001.

[85] Dan Shen, Genshe Chen, Leonard Haynes, and Erik Blasch. Strategies comparison for game theoretic cyber situational awareness and impact assessment. In *Information Fusion, 2007 10th International Conference on*, pages 1–8. IEEE, 2007.

[86] Philippe Smets. The combination of evidence in the transferable belief model. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 12(5):447–458, 1990.

[87] Philippe Smets and Robert Kennes. The transferable belief model. *Artificial intelligence*, 66(2):191–234, 1994.

[88] Duncan Smith and Sameer Singh. Approaches to multisensor data fusion in target tracking: A survey. *Knowledge and Data Engineering, IEEE Transactions on*, 18(12):1696–1710, 2006.

[89] Siddharth Sridhar and G Manimaran. Data integrity attacks and their impacts on scada control system. In *Power and Energy Society General Meeting, 2010 IEEE*, pages 1–6. IEEE, 2010.

[90] Alan N. Steinberg, Christopher L. Bowman, and Franklin E. White. *Revisions to the JDL data fusion model*. American inst of aeronautics and astronautics New York, 1998.

[91] Nils Svendsen and Stephen Wolthusen. Multigraph dependency models for heterogeneous infrastructures. *Critical Infrastructure Protection*, pages 337–350, 2007.

[92] George P Tadda and John S Salerno. Overview of cyber situation awareness. *Cyber Situational Awareness*, pages 15–35, 2010.

[93] University of Washington Power Systems Test Case Archive. 118 Bus Power Flow Test Case. IEEE Common Data Format, 1993. URL http://www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm.

[94] T. van Cutsem and M. Ribbens-Pavella. Critical Survey of Hierarchical Methods for State Estimation of Electric Power Systems. *IEEE Transactions on Power Apparatus and Systems*, PAS-102(10): 3415–3424, October 1983. doi: 10.1109/TPAS.1983.317838.

[95] Alexandre Veremme, Daniel Dupont, E Lefevre, and David Mercier. Belief assignment on compound hypotheses within the framework of the transferable belief model. In *Information Fusion, 2009. FUSION'09. 12th International Conference on*, pages 498–505. IEEE, 2009.

[96] Sicco Verwer, Mathijs De Weerdt, and Cees Witteveen. An algorithm for learning real-time automata. In *Proceedings of the Sixteenth Annual Machine Learning Conference of Belgium and the Netherlands (Benelearn)*, pages 128–135, 2007.

[97] Frans Voorbraak. A computationally efficient approximation of dempster-shafer theory. *International Journal of Man-Machine Studies*, 30(5):525–536, 1989.

[98] J.W. Wang and V.H. Quintana. A decoupled orthogonal row processing algorithm for power system state estimation. *Power Apparatus and Systems, IEEE Transactions on*, PAS-103(8):2337 – 2344, aug. 1984. ISSN 0018-9510. doi: 10.1109/TPAS.1984.318550.

[99] Duncan Watts and S Strogatz. The small world problem. *Collective Dynamics of Small-World Networks*, 393:440–442, 1998.

[100] Allen J Wood and Bruce Wollenberg. *Power Generation, Operation and Control*. John Wiley & Sons, 2006.

[101] Le Xie, Dae-Hyun Choi, Soummya Kar, and H. Vincent Poor. Fully Distributed State Estimation for Wide-Area Monitoring Systems. *IEEE Transactions on Smart Grid*, 3(3):1154–1169, September 2012. doi: 10.1109/TSG.2012.2197764.

[102] Tao Yang, Hongbin Sun, and A. Bose. Transition to a Two-Level Linear State Estimator — Part I: Architecture. *IEEE*

Transactions on Power Systems, 26(1):46–53, February 2011. doi: 10.1109/TPWRS.2010.2050078.

[103] Tao Yang, Hongbin Sun, and A. Bose. Transition to a Two-Level Linear State Estimator — Part II: Algorithm. *IEEE Transactions on Power Systems*, 26(1):54–62, February 2011. doi: 10.1109/TPWRS.2010.2050077.

[104] Lotfi A Zadeh. A simple view of the dempster-shafer theory of evidence and its implication for the rule of combination. *AI magazine*, 7(2):85, 1986.

[105] Majid Zandipour, Bradley J Rhodes, and Neil A Bomberger. Probabilistic prediction of vessel motion at multiple spatial scales for maritime situation awareness. In *Information Fusion, 2008 11th International Conference on*, pages 1–6. IEEE, 2008.

PUBLICATIONS

Journal:

G. Digioia, C. Foglietta, G. Oliva and S. Panzieri, "Aware on-line interdependency modeling via evidence theory," *International Journal of Critical Infrastructures*, To Appear

Book Chapters:

G. Digioia, C. Foglietta, G. Oliva, S. Panzieri and R. Setola, "Moving from looking to understanding: Situation Awareness and Prediction," In *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues* , CRC Press / Taylor & Francis eds., To Appear.

C. Foglietta, G. Oliva and S. Panzieri, "Online Distributed Evaluation of Interdependent Critical Infrastructure" In *Nonlinear Estimation and Applications to Industrial Systems Control*, Nova Pubblications eds., 2012.

Proceedings:

Y. Feng, C. Foglietta, A. Baiocco, S. Panzieri, S. D. Wolthusen, "Malicious False Data Injection in Hierarchical Electric Power Grid State Estimation Systems", Accepted at *ACM e-Energy* 2013

A. Di Pietro, C. Foglietta, S. Palmieri, S. Panzieri, "An experimental framework for impact assessment of cyber attacks on interdependent physical systems", *IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, 2013

G. Digioia, C. Foglietta and S. Panzieri, "An Agile Model for Situation Assessment: how to make Evidence Theory able to change idea about classifications", in *Proceedings of the International Conference on Information Fusion*, FUSION 2012, 2012

G. Digioia, C. Foglietta, S. Panzieri and A. Falleni, "Mixed Holistic Reductionist Approach for Impact Assessment of Cyber Attacks" *European Intelligence & Security Informatics 2012*, August, 2012

C. Foglietta, A. Gasparri, S. Panzieri, "Networked Evidence Theory Framework in Critical Infrastructure Modelin" *Sixth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, Fort McNair, Washington, DC, USA, March 19-21, 2012

G. Digioia, C. Foglietta, G. Oliva and S. Panzieri, "Countermeasures Selection via Evidence Theory," *6th International Conference on Critical Information Infrastructure Security* (CRITIS2011), 2011

Paolo Capodieci et al. , "Improving Resilience of Interdependent Critical Infrastructures via an On-Line Alerting System" *Proceedings*

of COMPENG 2010 - Complexity in Engineering, 2010

E. Ciancamerla, S. Di Blasi, C. Foglietta, D. Lefevre, L. Lev, M. Minichino, "Qos of a Scada system versus QoS of a power distribution grid" *10th International Probabilistic Safety Assessment & Management (PSAM) Conference PSAM 10*, June, 2010

E. Ciancamerla, C. Foglietta, D. Lefevre, M. Minichino, L. Lev and Y. Shneck, "Discrete event simulation of QoS of a SCADA system interconnecting a Power grid and a Telco network" *1st IFIP International Conference on Critical Information Infrastructure Protection*, September, 2010

E. Ciancamerla, S. Di Blasi, C. Foglietta, D. Lefevre, M. Minichino, L. Lev and Y. Shneck, "QoS of a SCADA system interconnecting a Power grid and a Telco network" *4th National Conference of Italian Association of Energy Management AIGE*, May, 2010

Technical Report:

L. Sciavicco, S. Panzieri, G. Ulivi, F. Pascucci, F. Moretti, C. Foglietta, P. Cicolin S. Pizzuti, "Realizzazione di una piattaforma integrata per il data fusion di segnali provenienti da sistemi sensoriali per applicazioni di smart city integrate nella rete della pubblica illuminazione," *Tech rep. Roma Tre. pag. 53*, ENEA, 11, 2011. (in italian)