**Model-Based Evaluation of the Impact of Attacks to the Telecommunication Service of the Electrical Grid**

# Critical Information Infrastructure Protection and Resilience in the ICT Sector

Paul Theron
*Resilience Studies Team, France*

Sandro Bologna
*AIIC, Italy*

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Editorial Director: Joel Gamon
Book Production Manager: Jennifer Yoder
Publishing Systems Analyst: Adrienne Freeland
Development Editor: Myla Merkel
Assistant Acquisitions Editor: Kayla Wolfe
Typesetter: Christina Henning
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com



Library of Congress Cataloging-in-Publication Data

Critical information infrastructure protection and resilience in the ICT sector / Paul Theron and Sandro Bologna, Editors.
pages cm.
Includes bibliographical references and index.
Summary: “This book brings together a variety of empirical research on the resilience in the ICT sector and critical information infrastructure protection in the context of uncertainty and lack of data about potential threats and hazards”--Provided by publisher.
ISBN 978-1-4666-2964-6 (hardcover) -- ISBN 978-1-4666-2965-3 (ebook) -- ISBN 978-1-4666-2966-0 (print & perpetual access) 1. Telecommunication--Safety measures. 2. Emergency management. I. Theron, Paul, 1957- II. Bologna, Sandro.
TK5102.85.C75 2013
384.068’4--dc23

2012037381

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

# Chapter 11
# Model-Based Evaluation of the Impact of Attacks to the Telecommunication Service of the Electrical Grid

**M. Beccuti**
*Università di Torino, Italy*

**S. Donatelli**
*Università di Torino, Italy*

**S. Chiaradonna**
*ISTI – CNR, Italy*

**G. Dondossola**
*RSE S.p.A., Italy*

**F. Di Giandomenico**
*ISTI – CNR, Italy*

**G. Franceschinis**
*Università del Piemonte Orientale, Italy*

## ABSTRACT

*This chapter is devoted to the study of the consequences of cyber-attacks to the telecommunication service of the electrical grid, which is an essential service for the grid control system. It is up to the control system to ensure that even very large power systems are kept in equilibrium even in presence of power contingencies. This chapter considers cyber-attacks of the Denial of Service (DoS) type, occurring while the electrical grid is already facing an electrical failure that requires a load shedding strategy. Using a model-based approach that uses the rich and flexible formalism provided by the tool Möbius, it is possible to investigate the interplay between an attack to the telecommunication service and the state of the grid in a number of different situations and for different characterizations of the DoS behaviour and severity. The formalism used allows to associate a (stochastic) duration and/or a probability to the events happening in the system, so as to take into account the variability in attacks' behaviour, leading to a quantitative characterization of the impact of a DoS attack to the electrical grid.*

DOI: 10.4018/978-1-4666-2964-6.ch011

## INTRODUCTION

Energy Power Systems (EPS) can be considered as the composition of two major elements: the Energy Infrastructure (denominated in the following Energy Infrastructure EI) and the information and communication technology distributed control system (denominated in the following Information Infrastructure II) that supervises the EI. The supervision and control may be impaired by malfunctions in the underlying telecommunication system, or in some node of the control system itself. Even assuming that the II is working, we have to consider the possibility that cyber attacks may alter its correct behaviour: this may be due to a specific malware that alters the behaviour of the EI control algorithm, or the value of the control data transmitted, but it may be also due to an attack to the telecommunication network, provoking message losses and/or delays which may lead to a partial malfunctioning of the control system. Lost or delayed messages may not be so crucial when the EI is working in normal status, but they may have drastic consequences when the EI is facing an electrical failure. Since EPSs provide vital services to a variety of activities governing people life, it is of relevant importance to assess the possible cascading effects that failures in the II control subsystems may have, when they occur in critical scenarios of the EI.

Indeed an important step towards the design of a reliable service, consists in clarifying the (inter) dependencies between the electrical and information infrastructures. In particular it is important to investigate the possible consequences of a failure to one or more nodes of the II distributed control system, or to the telecommunication network supporting the information exchange among the distributed control system components at different levels in the EI control hierarchy. The large space of possible critical situations need to be explored selecting a set of representative scenarios (that should be enriched on the basis of the experience) and evaluating the possible behaviours as a function of the type of failure (e.g. those caused by an attack) and of the state of the EI when the failure comes into play. It is very important to have a reference framework to abstract out from the details of the specific scenario or experiment, recognize recurring patterns of cascading behaviour, and provide a quantitative evaluation of their impact.

Although the modelling of the types of failures that are characteristic of interdependent critical infrastructures has received increasing interest in the last years, after the large blackouts of electric power systems in 1996 and 2003, there is still no definite understanding on EPS interdependencies, and on the techniques to evaluate even the dependency between an II failure/malfunctioning and the services provided by the whole EPS. It is indeed of great importance for the utilities operating the infrastructures to have methods/tools for analysing threat impacts and technologies for avoiding, or limiting, most serious consequences.

Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book has characterized and analysed the risk of different types of cyber attacks to the II, which is a fundamental step in setting up ICT countermeasures, but a complete evaluation of the attack impact requires an evaluation of the consequences of a successful attack on the overall behaviour of the electrical grid. In this chapter we propose a framework to understand and evaluate the cascading effects of attacks to the telecommunication service that supports the distributed control system of an energy grid in critical scenarios (like in presence of a failure of a grid component). A model-based approach is chosen, due to its high flexibility in exploring a wide range of alternatives at a limited cost and in representing at different abstraction levels the various layers of the EPS hierarchy (e.g. transmission versus distribution, local versus regional and multiregional as proposed for example in (Beccuti, Chiaradonna, Di Giandomenico, Donatelli, Dondossola & Franceschinis, 2012), (Chiaradonna, Lollini & Di Giandomenico, 2007) and (Chiaradonna, Giandomenico & Nostro, 2011).

In particular a stochastic modelling approach has been pursued, that allows to represent randomness of physical faults and to model at a sufficiently high level of abstraction the effect of malicious attacks, as they propagate under variable network conditions. Moreover, model based approaches have the potential to support extensive experimentation on a wide variety of scenarios, analysing the infrastructures behaviour and their mutual interdependencies at different abstraction levels, depending on the aim of the study. A combination of analytical and simulation approaches may be applied to evaluate the indices of interest, measuring the severity of the consequences of a simultaneous occurrence of physical failures in the EI and a malfunction in the II control system (possibly caused by a cyber attack).

In this chapter we build on the model of EPS presented in (Chiaradonna, Di Giandomenico & Lollini, 2011), which defines a set of stochastic models representing in a rather faithful way (yet abstract enough to be tractable) both the electrical infrastructure evolution in presence of failures, and the control actions activated by the control system (both locally and at a higher level in the control hierarchy). The model is here enriched with a set of submodels that represent a cyber attack. We concentrate on DoS attacks, and consequently the model of the EPS includes also a rather detailed model of the DoS behaviour, both the DoS internal evolution (the DoS attack may increase or decrease in severity) and the effect on the messages exchanged by the control system (delayed or lost messages).

The model obtained can then be exercised with different parameters for the EI and the II behaviour, to investigate the impact of the DoS behaviour on the service delivered by the EPS. Due to the complexity of the model, the results have been collected using large sets of simulation runs. In particular in this chapter we report the experiments for a scenario in which the EPS has to execute a load shedding strategy due to an EI failure, as already described in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"*, and the electrical grid of reference is the IEEE RTS96 test grid.

Although this chapter concentrate on DoS attacks, the set-up of the interaction between the models of the attack and of the EPS is adequate for any type of attack that delays or deletes packets.

The rest of the chapter is structured as follows. First, background is provided by overviewing relevant literature on the study of dependencies, in particular in the case of electrical infrastructure. The proposed modelling framework is then described, with a two level approach: the logical scheme is described first, which identifies the components of the EPS and their interaction at a rather high level of abstraction, followed by a more detailed description of the specific models of the components and of their interactions. The modelling framework is finally exercised on the case study. A particular attention has been devoted to the choice of the parameters of the model, taking into account the indication of the experiments on DoS attacks reported in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book, both to parameterize the model and to define the performance indices of interest.

## BACKGROUND

Understanding the interdependencies among interacting critical infrastructures, as well as quantifying resiliency, security and robustness related indicators are tackled by a number of research initiatives (see (Chiaradonna, Di Giandomenico & Lollini, 2008) for an overview). A rigorous approach to analyse and understand how infrastructure sectors evolve, where they are vulnerable, and how they can be protected is presented in (Lewis, 2006).

The infrastructures interdependency issues have been tackled in several projects in Europe and the United States. The IRRIIS European project (IRRIIS) has devoted significant effort

to interdependencies analysis and modelling. A theoretical framework has been developed in (Nieuwenhuijs, Luiijf & Klaver, 2009), which views a Critical Infrastructure (CI) as a process and dependencies as response functions. Quantitative interdependency analysis, in the context of Large Complex CI, is presented in (Bloomfield, Buzna, Popov, Salako & Wright, 2009), where a discrete state-space, continuous-time stochastic process models the operation of critical infrastructure, taking interdependencies into account. Of primary interest are the implications of both the abstraction level of the model and its parameterization on the distribution of cascade sizes within and across infrastructures. The IRRIIS consortium has developed SimCIP (Simulation for CI Protection), an agent-based simulation environment for controlled experimentation, with the aim of providing insights on CI behaviour and their interdependencies (Klein, 2008). The proposed scenario considers the impact of EI failures on the ICT control system.

The CRUTIAL European Project (CRUTIAL) has dedicated significant efforts to the modelling of (inter)dependencies between the two infrastructures constituting an EPS (Electrical Power System): the power grid and its cyber controls. In the context of CRUTIAL, an innovative, modular EPS modelling approach, that considers separately the two constituting infrastructures but takes into account their interdependencies and allows to assess the impact of reciprocal failures, has been developed (Chiaradonna, Di Giandomenico & Lollini, 2011).

The National Science Foundation project TCIP, currently extended in TCIP-G (TCIP-G) with support from the Department of Energy and contributions from the Department of Homeland Security, focuses on securing the low-level devices, communication and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber attacks and/or power emergencies. As reported in (Sanders, 2010), quantitative and qualitative evaluation constitutes a major research effort in TCIP with investigations on means to model, simulate, emulate and experiment with the various subsystems in the power grid. Although interdependencies are among the aspects of interest in these studies, the major effort is devoted to cyber security, smart grid vulnerabilities and communication technologies.

A review of the work related to Smart Grid cyber security is presented in (Baumeister, 2010), which also includes security assessment methods spanning attack injection, simulation and probabilistic approaches.

Attack trees (Ten, Liu & Govindarasu, 2007), attack graphs (Lippman & Ingols, 2005 and Chapter *"Using Hybrid Attack Graphs to Model and Analyze Attacks against the Critical Information Infrastructure"* of this book*)* and access graphs (Hahn & Govindarasu, 2010) have been proposed for cyber security analysis in smart grids; such methods are directed to find ways in which an adversary can exploit vulnerabilities to break into a system and to assess the exposure level of the system to such attacks. An exposure metric to identify the set of security mechanisms required to protect the various information objects utilized within a grid has been proposed in (Hahn & Govindarasu, 2011). Other works have been directed to the analysis of structural vulnerabilities and the risk of cyber attacks. In (Bompard, Napoli & Xue, 2009), the authors conducted a structural analysis of the power transmission grid by applying a topological approach that extends the traditional topological metrics derived from complex network theory. This approach can be used to assess structural vulnerabilities in power systems in contrast with traditional, purely topological metrics. The impact analysis of control systems availability on managing power contingencies is not supported by this extended topological approach.

Also, a number of experimental testbeds have been set-up for security analysis of a variety of aspects related with smart grids, such as the work in (Coppolino, D'Antonio, Elia & Romano, 2011) concerning technologies for data collection, and

most of the literature reported in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book.

Differently from these approaches, we are not interested in identifiying the vulnerability paths and the success probability of the attack; rather, our objective is to analyze the consequences of the attacks on the ability of the system to preserve the correct operation.

Security and privacy challenges faced by the smarter electrical grids that are going to replace physical infrastructures in the near future are overviewed in (McDaniel & McLaughlin, 2009). Several attacks typologies are identified, and a national effort is advocated to investigate smart grid security, including the extensive evaluation of the security of these devices, both in the laboratory and in the field.

In (Beccuti, Franceschinis, Donatelli, Chiaradonna, Di Giandomenico, Lollini et al., 2009) and (Beccuti, Chiaradonna, Di Giandomenico, Donatelli, Dondossola & Franceschinis, 2012) the effect of a Denial of Service (DoS) attack during the execution of an emergency procedure recovering from a power grid failure scenario has been evaluated using stochastic models: the approach is similar to (Bloomfield, Buzna, Popov, Salako & Wright, 2009), but it is specifically tailored to EPS and allows to deal with a more detailed representation of the major components and dynamics of the power grid and related ICT controls. Considering the effect of attacks to the ICT on failure propagation in the EPS, the scenario is complementary with respect to the IRRIIS ones. The work in this chapter extends the studies in (Beccuti, Chiaradonna, Di Giandomenico, Franceschinis, Donatelli & Dondossola, 2012) in two directions: i) by proposing novel models for the attacks affecting the control infrastructure, and ii) by embedding in the developed models more faithful parameters characterizing the attacks behaviour, as determined by experimental studies documented in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book.

## THE MODELING FRAMEWORK

The modelling framework is here described with a two-level approach: the logical structure of the model is presented first, and then the specific models are discussed in more detail.

The logical structure depicts how the physical electrical grid is modelled, and how the control system is taken into account, as well as the characteristics of the DoS attack have been considered, and how the model of the attack influences the model of the control.

The overall model has been developed with a compositional approach, well supported by the Möbius tool (Daly, Deavours, Doyle, Webster & Sanders, 2000) used for the modelling activity.

Thanks to the features offered by Möbius, a modular approach to models development has been possible, with the definition of atomic models capturing the structure and behaviour of basic EPS components and related phenomena, then properly composed to obtain the overall EPS model.

The model will be the exercised on a reference scenario, and it has been tailored with an abstraction level adequate to represent all the relevant aspects of the scenario. We shall therefore describe it first, to then explain the modelling framework, articulated in a description at the logical level, followed by a more detailed explanation of each model component.

### Reference Scenario

We consider an EPS system in which, in emergency conditions, the Transmission System Operator (TSO) is authorized by the Distribution System Operators (DSO) to activate load shedding activities on the Distribution Grid to actuate defence/recover actions. This is exactly the same scenario considered in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book, depicted in Figure 5 (of the same chapter), that we summarize here for ease of reference. The structure of the EPS system (ICT control and power grid elements controlled by) is also described in the same chapter, with the support of Figure 3.

The TSO Control Centre monitors continuously the EPS and when it detects a potentially dangerous condition that can be recovered with appropriate load shedding strategies (applied to specific areas of the grid), it chooses a subset of DSO SubStations (SSs) from the list of DSO SSs participating in the emergency plan, and sends the requests of preventively arming these DSO SSs. The request is sent to their DSO Control Centers (CCs), through a shared communication channel. Then the DSO CC forwards the arm request to the required DSO SSs, and returns the status of the substations to the TSO CC.

At the same time, a special TSO substation called TSO sentinel (usually a TSO node located in a strategic point of the grid) independently monitors the EI status to quickly detect if the potential emergency condition is evolving into a real emergency situation. When real emergency situation is detected the TSO sentinel sends the trip command to all the DSO SSs participating to the emergency plan; however only the DSO SSs that have been previously armed will be actually detached. In the period between the detection of a potential emergency and its evolution towards a new status, the TSO sentinel periodically sends test packets towards the detachable DSO SSs. If an armed DSO SS does not receive three consecutive test packets, it automatically disarms itself. Disarming also occurs after 20 min from the arming command if no trip command is issued by the sentinel.

## Logical Structure of the EPS Components and Characterization of the DoS Attack

The EPS components considered are those more deeply involved in the interaction between II and EI, specifically in presence of a DoS occurring while the EPS is experiencing one or more electrical failures. The scenario of EPS operations involves both Transmission and Distribution System Operators (TSO and DSO), but it considers as target of the DoS attack only the communication channel between a DSO control centre (DSO CC) and its controlled DSO substation (DSO SSs). Here we describe the logical EPS components and attack behaviours considered in the models, as well as their interaction schema.

### Logical Scheme of EI

EI represents the electric infrastructure necessary to produce and transport the electric power towards the final users. As already considered in previous studies the main elements that constitute the power grid are: generators, substations, loads and power lines (which also logically include breakers and protections connected to the power lines). One or more generators can be located inside the power plants. The energy produced by the generators is then adapted by transformers, to be conveyed with minimal dispersion, to the different types of end users (loads), through different voltage level power grids. The power lines are components that physically connect the substations with the power plants and the final users, and the substations are structured components in which the electric power is transformed and split over several lines. In the substations there are transformers and several kinds of connection components (bus-bars, protections and breakers).

### Logical Scheme of II

The Information Infrastructure implements the control system and its main purposes are: (1) to reduce the out-of-service time of generators, power lines and substations (availability); (2) to enhance quality of service (through frequency and voltage regulation); (3) to optimize generators and substations management. To these aims, II performs the following activities: (a) remote control of the electric infrastructure (it receives data and sends commands); (b) coordination of the maintenance (it plans the reconfiguration actions that can affect generators, substations, loads and lines); (c) collection of the system statistics.

Among the several logical components composing II, we focus the attention on the TSO and DSO components, since a failure of these logical components can affect a large portion of the grid, eventually leading to service interruptions of wide geographical areas and large black-out phenomena.

In details, the operations performed by the II control system are modelled considering two levels of abstraction on the basis of the locality of the EI state considered by the II to decide on proper reactions to disruptions.

Each level is characterized by an activation condition (that specifies the events which enable the II reaction), a reaction delay (representing the overall computation and application time needed by II to apply a reconfiguration) and a reconfiguration strategy (RS), based on generation re-dispatch and/or load shedding.

For each level, a different reconfiguration function is considered, to represent the effect on the electrical grid of the reactions of II to an event that has compromised the electrical equilibrium of EI, when only the state local to the affected EI components is considered. They are called RS1() and RS2().

RS1 is performed by the control units associated with the EI components (e.g. TSO Sentinels, DSO SubStations) and, because of the limited information necessary to compute its output, it is fast in providing its reaction. In the current implementation, the output of RS1 is obtained as the solution of a system of power flow equations that minimize a simple cost function, indicating the cost incurred in having loads not satisfied and having the generators producing more power. Observe that the reconfiguration strategy RS1 is applied immediately.

RS2 is performed by TSO CC through the DSO CC which sends the arming command to the selected DSO SS, and represents the effect on the regional transmission grid of the reactions of II to an event that has compromised the electrical equilibrium of EI, when the state of the whole EI system under the control of II is considered.

Therefore RS2 is determined on the global EI state and reacts in a longer time. In the reference scenario, it models the DSO SS arming as two asynchronous processes. The arming operation is immediately activated when an EI fault happens, but it requires more time than RS1 to be accomplished. Initially, the set of DSO SSs to be involved in the load shedding strategy is derived by solving an optimization problem to minimize the change in generation or load shedding, under additional system constraints, as described in (Romani, Chiaradonna, Di Giandomenico & Simoncini, 2007).

Then the transmission of arming request to the selected substations is explicitly modelled considering the behaviours of TSO CC, DSO CC, and DSO SS.

## DoS Attack Characterization

We do not model the DoS attack per se (generation of an high number of messages sent to a given target, as done for example in the testbed exposed in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book), but the effect of the attack on the communication systems in terms of lost or delayed messages. This is an adequate abstraction level for our study since our objective is not to study the DoS behaviour, but the consequences of a DoS attack (and therefore of a malfunctioning communication network to the services provided by a power grid). We shall therefore assume that a DoS alters the behaviour of the communication channel by inducing lost and delayed messages, and that the amount of lost or delayed messages, and the actual delay, does depend on a notion of "severity level" of the DoS: the more severe level, the more packets are lost and delayed, and longer delays are experienced. The DoS is a dynamic process: its severity may increase or decrease over time.

The effect of DoS occurrence is studied under emergency conditions (e.g. line failure, loss of generation, switching errors, etc.), when recovery

actions have to be performed under strict real time constraints to avoid the fault propagation within the EI.

In this context, different behaviours can be envisaged depending on *when* the DoS occurs. For instance, a DoS attack starting before an arming request has been issued towards a given DSO SS may impair the possibility of the DSO SS to execute the trip command (only armed substation may detach themselves from the grid). Instead, if a DoS attack takes place when the substation is armed, the attack may deny the successful execution of the periodic testing with the consequent automatic disarming of the DSO SSs. Finally, the DoS may occur just before sending the trip command, which implies that the arming command have been already sent (and received, since there was no active DoS at the time of arming): since we assume that the trip command is sent on a separate channel, not affected by the considered DoS, then we can assume that it reaches the selected substations, that correctly perform the trip command. The global effects of the considered DoS on the whole EPS clearly depend on the number and position of the DSO SSs affected by the attack and on the pattern and intensity of the DoS process. Since in our experiments we assume a DoS attack on the communication channel connecting DSO CC to its DSO SSs, the time needed to arm DSO SSs can increase substantially depending on the DoS severity.

Indeed arming commands, sent by DSO CC to DSO SS, can be lost or delayed due to the DoS attack effect. Instead, the trip command is sent to all the DSO SSs asynchronously with respect to arming requests, but only the armed DSO SSs will be involved in EI reconfiguration. In this way a load shedding strategy is terminated correctly (EI stability is restored) only if all the DSO SSs selected to be armed have received an arming request; otherwise a further arming and trip commands are performed.

## EI and II Interaction

To better understand the interplay of EI and II in presence of a DoS attack we shall consider the sequence of events involved in two possible interactions between the model of the EI and that of the II. The first interaction happens when the RS1 function finishes and its result (in terms of local reconfiguration actions) is applied directly to the EI; the second happens when the RS2 function finishes and the load shedding strategy is applied to stabilize the EI.

Note that in our scenario, RS1 is not influenced by the modelled DoS attack since it is a local reconfiguration; while the success of RS2, representing a global reconfiguration, depends on the number of stations that are reachable, and therefore may heavily depend on the DoS severity level.

The timed evolution of the EI and II models is shown in Figure 1, in a situation in which a EI failure occurs at time 0 while the communication channel between DSO CC and DSO SSs is not affected by a DoS attack. In this case, all the DSO SSs involved in the load shedding strategy will be correctly armed before applying the trip command, so that the EI will be stabilized with high probability.

Figure 2 describes instead the timed evolution of the EI and II models when an EI failure happens at time 0 and a DoS attack occurs on the communication channel between the DSO CC and the DSO SSs. In this context, only a subset of the DSO SSs, which should be armed, will be correctly armed when the trip command is issued.

Indeed, in presence of a DoS of high severity (or of a DoS that has reached a high severity level), an arming request sent by the DSO CC to a DSO SS can be lost or delayed so heavily so as to arrive after the trip command has been received by the DSO SS. Obviously this has an impact on the success of the load shedding strategy; if the procedure is not successful another RS2 function

*Figure 1. Timed evolution of the EI and II upon a single EI failure without DoS attack*

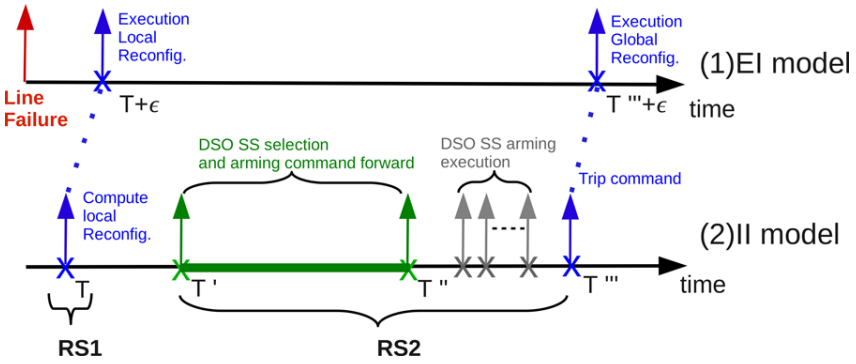
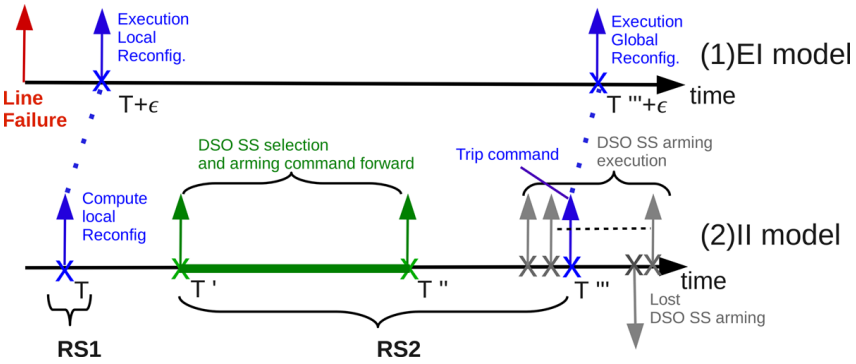



*Figure 2. Timed evolution of EI and II upon a single EI failure in presence of DoS attack on the communication channel between the DSO CC and DSO SSs*




is immediately re-started to stabilize the EI. However, this introduces a delay in stabilizing the EI, which could lead to a cascading effect: new high voltage lines in the power grid could fail increasing the EI severity status and/or giving rise to a large blackout.

## Models Description

All the models developed have been described using the Stochastic Activity Network (SAN) formalism defined within the tool Möbius (Daly, Deavours, Doyle, Webster & Sanders, 2000). SAN is a formalism that extends the Stochastic Petri Net and it is meant for modelling the behaviour of discrete event dynamic systems, in particular in terms of their possible stochastic behaviour (probabilistic choices and random delays associated to events). The system state is represented through the *marking* of SAN places: there are two types of places, *standard* places, that have an associated state expressed as a non-negative integer (called marking) and *extended* places, whose state is a variable of any type recognized as a legal type in the C language. A place graphically appears as a circle: blue circle for standard place and orange for extended one.

An activity (also called transition) may take place (fire) when its condition (defined on a subset of the model places) is true. The effect of the firing of an activity is to modify in some way the marking of the places. In the SAN formalism, an activity can be immediate (graphically a bar) or timed (graphically a thin box): immediate fire in zero time while timed ones fire after a random/deterministic delay has elapsed since its enabling.

An activity of any kind is enabled by a particular condition on the marking of a set of places. For simple conditions involving only standard places this can be modelled by directly connecting such places with the activity through properly oriented arcs.

Another way to express the enabling condition of a certain activity are the input gates. An input gate is connected to an activity and to a subset of standard or extended places; the input gate is characterized by two expressions: 1. a *predicate,* a Boolean condition expressed in terms of the marking of the places connected to the gate; if such condition holds, then the activity connected to the gate is enabled; 2. a *function* expressing the effect of the activity firing on the marking of the places connected to the gate.

Besides input gates, a SAN model can contain output gates. An output gate has to be connected to one activity and to a set of standard or extended places; and it specifies through a function the effect of the activity firing on the marking of the places connected to it.

Hence, the marking enabling a given activity can be expressed by means of oriented arcs, or by means of an input gate. Input and output gates graphically appear as left oriented red and right oriented black triangles, respectively.

In a SAN model, it is possible to set several firing cases for an activity; each case corresponds to a different effect of the firing and has a certain probability: when the activity fires, one of its cases is chosen at random. A case graphically appears as a small circle close to the activity; from the case an arc is directed to an output gate or to a set of standard places.

Finally a SAN model can be expressed using *hierarchical modelling paradigm,* so that it is possible to specify the behaviour of each individual component (*atomic model*), and then combine such components to create a model of the complete system through the Replicate and Join operators.

We shall now proceed to a general description of the models that compose the whole SAN model of the EPS, to then provide a more detailed description for the models that takes into account the specific scenario of a load shedding strategy and the behaviour of a communication channel subject to a DoS attack.

## The EPS SAN Model

A modular and compositional approach is employed to model an electric power system. A number of atomic models have been developed to represent both EI and II logical components, as identified in the previous Section, and their interactions in presence of malfunctions affecting one or both infrastructures. Such atomic models, implemented through the Stochastic Activity Networks (SAN) formalism, have been already presented in previously published papers (e.g., (Chiaradonna, Lollini & Di Giandomenico, 2007) and (Chiaradonna, Di Giandomenico & Lollini, 2011)). Therefore, we shortly recall them in this chapter, but without details. They are the models representing:

- The generic power line with connected transformers;
- The generic protection mechanisms and breakers connected to the two extremities of the power line;
- The automatic evolution (autoevolution) of the electrical infrastructure when an event modifying its state occurs;
- The computation and application of the local reconfiguration strategy RS1(), and the computation of the global reconfiguration action RS2();
- A node in the grid (generator, load or substation) and the associated control and regulation mechanisms (TSO sentinel and DSO SS);
- The TSO CC system, where the regional reconfiguration strategy RS2() is applied, and the DSO communication network.

While we basically maintained the above recalled models in the current EPS modelling framework, we extended the models related to the II infrastructure for what concerns the protocols addressed by the scenario to apply the emergency plan (arming requests) and the severity of the attacks to the DSO net, in particular all the models associated to the last two sets of submodels listed above have been modified with respect to the one proposed in (Chiaradonna, Di Giandomenico & Lollini, 2011), to appropriately take into account the reference scenario.

The newly developed models allow us to represent with higher accuracy the attacks processes, which have impact on the time to the application of the global reconfiguration function RS2(), resulting in an improved accuracy of the measures assessed through the developed EPS modelling framework.

## The Model Components Relevant for the Scenario

The II additional behaviour that takes into account the protocol associated to the load shedding scenario is modelled through four atomic models (TSO CC and DSO CC, communication channel, DSO SS and DoS attacker) shown as separate entities in Figure 4, while Figure 3 accounts for their interaction through common places.

The whole II model is obtained in two steps. First the DSO SS and network models are joined together through superposition on place *Rec*, which is then replicated as many times as the number of DSO SSs. Secondly the obtained model is joined with the models of TSO/DSO CC and of the DoS attacker through superposition on places *SeverityDos* and *Packet.*

Before describing each component in detail, let us recall some graphical aspects of the SAN formalism used: standard places are depicted in blue (dark in black and white) like places *arm* and *Buffer_Out* in Figure 4, extended places are depicted in orange (light color in black and white), like place *Packet* in the same Figure, which is an extended place encoding a short vector with dimension equal to the total number of DOS SSs. All activities of Figure 4 are timed (blue bar), with an associated stochastic or deterministic delay. Input gates are depicted as red triangles (light colour in black and white), while output gates are black triangles. The predicate and the function implemented by the gate are an integral part of the model definition, although they are not shown on Figure 4 for the sake of readability. For example the predicate for the input gate *isArm* is*:* "marking of *arm* must be different from 0 and marking of *Buffer_Out* cannot be greater than the predefined buffer size"; while its function decreases by one the marking of place *arm*. An example of the use of cases is illustrated by the transition *Sent* of Figure 4: there are two firing cases that model the possibility of losing or not an arming command, depending on the DoS severity level (marking of the standard *SeverityDoS* place).

*Figure 3. Composition scheme of the submodels in Figure 4*

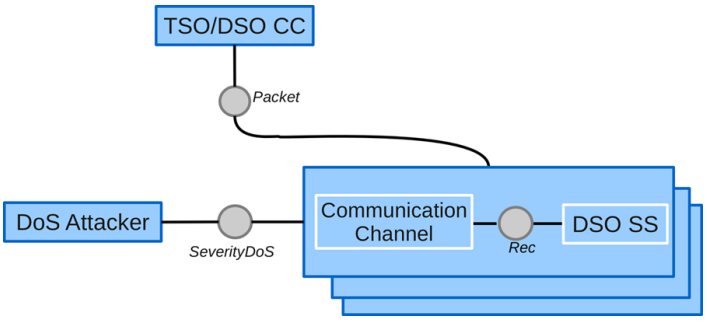
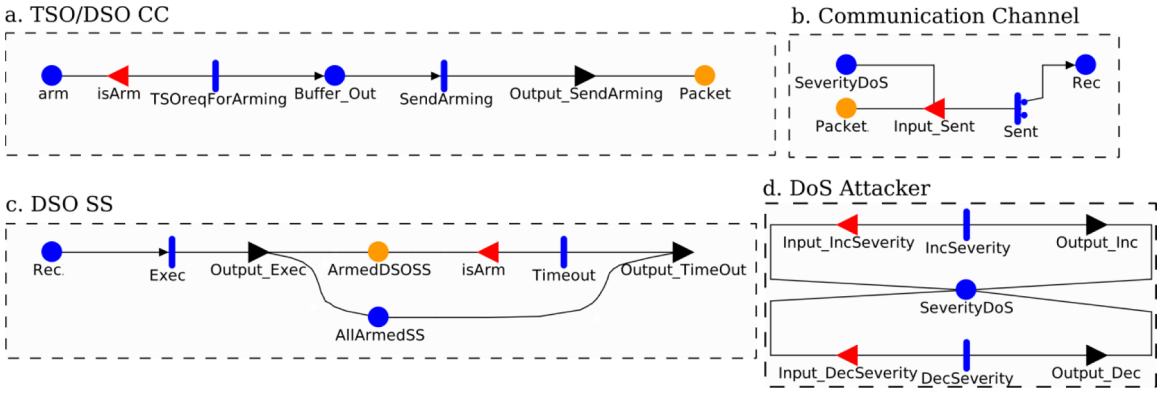


*Figure 4. SAN atomic models of the components involved in the load shedding process and of the DoS attack*




The model in Figure 4a represents the arming process that involves the TSO CC and DSO CC. When the place *arm* is marked due to the detection of an EI fault (interaction with the II submodel), then the arming process is started: this is represented by activity *TSOreqForArming*, modelling the TSO CC choice of which DSO SSs will be involved in the arming process and their notification to the DSO CC.

After *TSOreqForArming* firing the DSO CC sends the arming commands (activity *sendArming*) to its DSO SSs, which have been selected by the TSO CC. These commands are sent to the corresponding DSO SSs through the communication channel modelled by the model in Figure4b. The extended place *Packet* contains all the arming commands, which are waiting for being transmitted from the DSO CC to the DSO SSs; each command contains the id of the destination DSO SS. These arming commands can be lost or delayed (activity *Sent*) depending on the DoS attack severity (place *SeverityDoS*). A received command is stored in the input buffer (place *Rec*) of the corresponding DSO SS model.

The model of the behaviour of a DSO SS is modelled in Figure 4c. When an arming command is received in place *Rec,* the DSO SS arming is executed; this is modelled by the firing of activity *Exec,* which changes the marking of place *ArmedDSOSS*. Observe that place *AllArmedSS* is used to count the number of DSO SSs correctly armed and it is shared among all the DSO SS submodel replicas. Activity *Timeout* models a time-out after which an armed DSO SS is disarmed.

The DoS attack model is shown in Figure 4d, where the marking of place *SeverityDoS* represents the different DoS severity levels (i.e. $L_0$ is the lowest severity level,..., $L_{Max}$ is the highest severity level). *Activities IncSeverity* and *DecSeverity* are used to increase or decrease the DoS severity respectively. During the simulation, these two activities can be disabled thanks to two boolean parameters so that we can consider situations where the DoS severity can either decrease or increase or both.

## Models Interaction

The existing EPS modelling framework and the additional models, created for taking into account the scenario of interest, interact through common places shared between the SAN models that are composed by using rep and join operators. Figure 3 already describes the interaction between the components of the DoS SAN model. The composed model interacts with two additional SAN

submodels that are part of the overall EPS model. They are called RS and RTS and represent respectively the evaluation of RS2 and the application of the RS2 reconfiguration.

The extended place *ArmedDSOSS* is used by the RTS component to decide if an RS2 configuration can be applied, if all the stations involved in the new reconfiguration are armed, or not, and if at least one station involved in the reconfiguration is not armed. In this latter case a new evaluation of the reconfiguration of RS2 and the arming requests of the corresponding stations involved in the reconfiguration could be needed. The information about the stations that are not armed (which cannot therefore be involved in the evaluation of an RS2 configuration) is obtained by the RS submodel through common places shared between the RTS and RS components. Place *arm* is set to 1 by the SAN RS to trigger a new request of arming. The output gate *SendArming* sets to 1 all the items of the array Packet, corresponding to the stations to arm, based on the results of the linear programming problem solved in the RS submodel. This information is shared through an extended common place *deltaP_RS2* (that is not shown in Figure 4).

## CASE STUDY AND RESULTS DISCUSSION

The modelling framework developed in the previous Section has been exercised on a case study, to illustrate its features under interesting combinations of failures affecting the power grid infrastructures and attacks of different severity affecting the control infrastructure.

### EI Grid

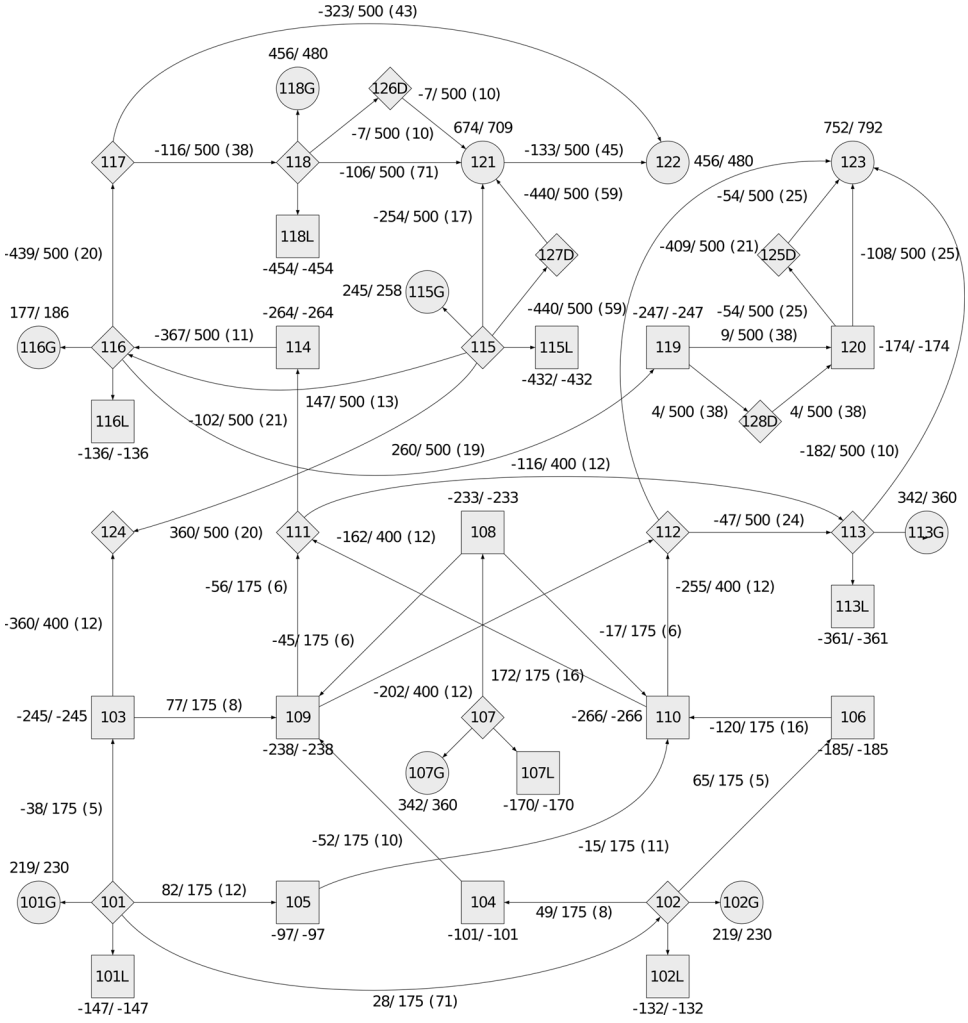
We used the IEEE Reliability Test System - 1996 (RTS- 96), described in (IEEE RTS, 1996), as the reference power grid for our analysis. This power grid has been used in a number of power system reliability evaluation studies, including those already performed by the authors of this paper. The configuration we consider is shown in Figure 5. It is composed of 42 nodes (of which 10 are generators and 17 are loads) and 56 lines. In the figure, label "$\mathbf{P_i/P^{max}_i}$" associated with the generators (circles) represents the initial (active) power $\mathbf{P_i}$ and the maximum power that the generator $\boldsymbol{i}$ can supply $\mathbf{P^{max}_i}$. Label "$\mathbf{D_i}$" associated with the loads (squares) represents the power demand (constant over time) of the load $\boldsymbol{i}$. Label "$\mathbf{F_{ij}/F^{max}_{ij}}$" associated with the lines represents the initial power flow $\mathbf{F_{ij}}$ through the line **(i,j)** and the maximum power flow $\mathbf{F^{max}_{ij}}$ that a transmission line can carry without incurring in overloading. A negative $\mathbf{F_{ij}}$ value means that the current is flowing in the opposite direction of the corresponding arrow. Also, in brackets it is shown the susceptance of each line. Note that the values for $\mathbf{D_i}$ and $\mathbf{P^{max}_i}$ have been assigned so as to intensify the stress of power lines, which carry a power flow closer to the maximum possible before overloading, to analyse the impact of attacks in rather critical conditions from the electrical point of view.

### II Model

In the II model we have considered a system composed by a single TSO CC and DSO CC, and 27 DSO SSs, resulting in a large SAN model with 177 places (most of which are complex places) and almost one hundred activities. For what concerns the parameter estimation of the activity delays we have used information reported in the literature (e.g. for activity *Timeout* in Figure 4c) or estimated through specific experiments performed on the testbed presented in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book.

For the TSO CC and DSO CC model *TSOreq-ForArm* is defined as a deterministic activity with deterministic delay equal to 8 minutes and *SendArming* fires with a random delay characterized by an Erlang probability distribution with 6 phases, each with mean sojourn time 0.0025 sec (rate 400), resulting in an average delay of 0.015s.

*Figure 5. Diagram of EI grid corresponding to the RTS96 test grid (generators are circles, loads are squares and substations are rhombi)*




In the network model activity *Sent* fires with a random delay distributed according to an hyper-exponential distribution that allows to account for the randomness of the communication time in presence of a DoS attack. It is characterized by a probability $p$ and two rates $\lambda_1$ and $\lambda_2$ (selected with probability $p$ and $1-p$ respectively); the three parameter values depend on the reached DoS severity level (i.e. $L_0$,...$L_5$) as shown in Table 1. For this activity the firing cases (deciding whether the packet is lost) are defined in terms of a Packet Loss Probability parameter, that also depends on the DoS severity level as reported in the same table (last column).

The parameter values characterizing activity *Sent* (delay and loss probability) can indeed be derived from the measures obtained through the experiments performed on the testbed as described in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book. We provide some hint on a possible approach to estimate the parameters from measures similar to those illustrated in Figures 6, 7 and 8 of Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"*. The loss probability can be derived by combining the information on frequency and duration of congestion periods and the percentage of lost messages in normal conditions and under congestion. In

*Table 1. Transmission delay and packet loss probability associated with each DoS severity level*

| DoS Severity | P | $\lambda_1$ | $\lambda_2$ | Packet Loss Probability |
|---|---|---|---|---|
| $L_0$ | 0.01 | 2.000 | 10 | 0.000 |
| $L_1$ | 0.50 | 2.000 | 10 | 0.010 |
| $L_2$ | 0.70 | 0.100 | 2 | 0.035 |
| $L_3$ | 0.80 | 0.050 | 2 | 0.052 |
| $L_4$ | 0.85 | 0.016 | 2 | 0.062 |
| $L_5$ | 0.95 | 0.012 | 2 | 0.078 |

order to correlate the packet loss probability with the DoS severity level it is necessary to repeat the experiments illustrated in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* several times under stable perturbation due to the traffic coming from the DoS attack. The delay could be derived from the inter message time measure introduced in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"*, and it should include the interaction between the retransmission of packets at the transport protocol level and the application level retransmission policy in case of missing acknowledge of control messages.

In the DSO SS model activity *Exec* fires with a random delay with average 0.2s characterized by an Erlang probability distribution with 4 phases, each with delay 0.05s (i.e. with rate 20); *Timeout* is a deterministic activity with delay equal to 20 minutes.

Finally, activities *IncSeverity* and *DecSeverity* in the DoS attacker model fire with a random delay characterized by a negative exponential probability distribution with rate 0.001.

Again, the parameter of the activities that describe the evolution (increase/decrease rate) of the DoS severity should be built from the data measured on several experiments emulating the same type of DoS attack under the same initial condition through the testbed, as explained in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"*. An histogram could be built showing the packet loss rate and average packet delay experienced in predefined intervals of time (taken since the start of the attack) while the DoS is actually increasing or decreasing. In general, deriving model parameters from the measures is a delicate task that may require several iterations for achieving reasonable accuracy: the steps for each iteration are (1) measurement, (2) parameters estimation from measured values, (3) validation of the effect induced by the estimated parameters values on the model behaviour (i.e. consistency check of some model derived measure with corresponding testbed measures); the last step may lead to more detailed measure requirements or adjustment of the parameters estimation procedure, or even to a model update (since this fitting with the measured data mat require a change in the level of detail of the model description).

As we shall see in the simulation results section, the measures may also be given as a *range* of realistic values for the model parameters: these may then be used to perform sensitivity analysis of the dependability measures of interest for a selected set of parameter values.

## Measures of Interest

Since the EPS is modelled as a stochastic process, the electrical energy provided to the final users (**i**th load **P**i) and the electrical energy required by the final users (**i**th demand **D**i) are random variables. Therefore, all the measures of interest we consider are the mean of random variables defined as a function of **P**i and **D**i. During the experiment it is assumed that these parameters do not change. The main measure of interest we consider in this chapter to assess the impact of cyber attacks in situations where the EI is affected by malfunctions, is $UD_{DoS}$, defined as the percentage of the power demand that, on average, is not met in the interval [0**; t**] (UD stands for "Unsatisfied Demand", see definition in Table 2). $UD_{DoS}$ is a measure of the service interruption, defined as the mean of the load shed during the period [0**; t**] (i.e., the total

unsatisfied load) divided by the total power demand in the same period. It provides an indication of the system operator satisfaction. The measure is computed through a transient analysis of the SAN overall model (obtained by composing the models presented in the previous Section).

This measure has been evaluated for different line failure initial events, and different communication network performance (from the most critical case where no substation is reachable, to the most favourable case in which all commands are delivered to the selected substations in due time, passing through intermediate dynamic situations due to a DoS attack in either increasing or decreasing phase). A sensitivity analysis has also been performed, as function of the delay distribution parameters assigned to activity *Sent*.

Other measures of interest are those characterizing the impact of an attack. In particular it can be of interest to estimate the expected value of the following two possible impact indicators defined in Chapter *"Cyber Risks in Energy Grid ICT Infrastructures"* of this book. The first one is

$$\gamma^j = n_j / m$$

where $n_j$ is the number of DSO SSs not armed due to the DoS attack (for a given severity evolution scenario *j*) and *m* is the total number of DSO SSs addressable by the load shedding application (according to the RS2 strategy). The second one is instead:

$$\gamma^i = P_i / P$$

where $P_j$ is the amount of load still connected due to the DoS attack (for a given severity evolution scenario *j*) preventing the arming of $n_i$ DSO SSs; *P* is the total amount of Load to be disconnected (according to the RS2 strategy).

In the simulation experiments the measure corresponding to the impact indicator $\gamma^j$ is $NA_{DoS}$ (see definition in Table 2).

*Table 2. Performance indices, acronyms and definition*

| Name | Definition |
|---|---|
| **Performance indices** | |
| $UD_{DoS}$ | $\frac{E\left[\sum_i \Delta P_i^{DoS}\right]}{E\left[\sum_i \Phi_i^{DoS}\right]}$ |
| $NA_{DoS}$ | $\frac{E\left[N_{DoS}\right]}{E\left[A_{DoS}\right]}$ |
| $\Delta P_i^{DoS}(u)$ | $\int_0^\infty \left(D_i^{DoS}\left(u\right) - P_i^{DoS}\left(u\right)\right) du$ |
| $\Phi_i^{DoS}(u)$ | $\int_0^\infty D_i^{DoS}\left(u\right) du$ |
| $D_i^{DoS}\left(u\right)$ | $D_i\left(u\right)$, if, at time *u*, the DoS is active or its effects are not yet removed |
| | 0, otherwise |
| $P_i^{DoS}\left(u\right)$ | $P_i\left(u\right)$, if, at time *u*, the DoS is active or its effects are not yet removed |
| | 0, otherwise |
| $N_{DoS}$ | The total number of DSO SSs not armed due to the DoS attack, during the period the DoS is active or its effects are not yet removed |
| $A_{DoS}$ | The total number of DSO SSs addressable by strategy to which the arming request has been sent, during the period the DoS is active or its effects are not yet removed |
| **Acronyms** | |
| LCSU | All LCS Unreachable |
| LCSR | All LCS Reachable |
| TDDS | Time Depending Decreasing Severity |
| TDIS | Time Depending Increasing Severity |

## Analysis of the Simulation Results

In the following, we discuss the results of the analyses performed. All the results have been obtained through simulations consisting either of

*Figure 6. $UD_{DoS}$ and $NA_{DoS}$ as a function of the DoS behaviour for different failed power lines*

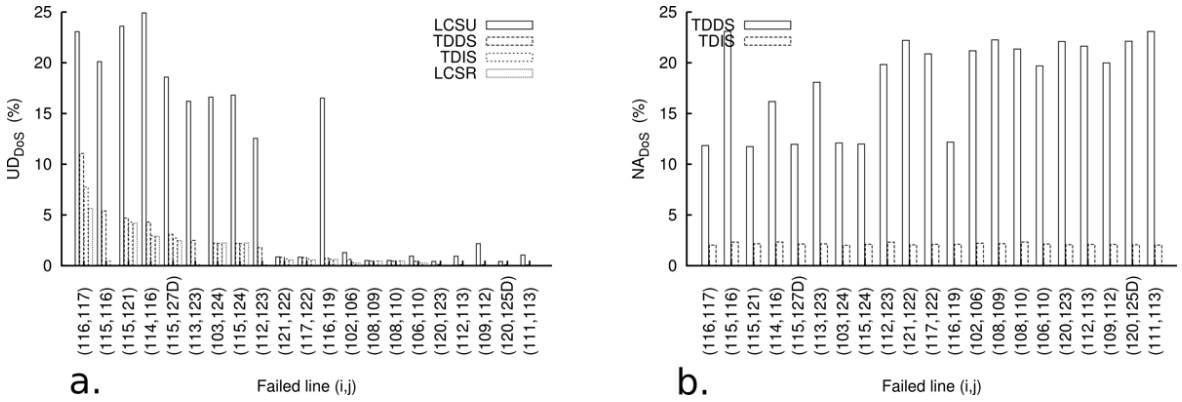



*Figure 7. $UD_{DoS}$ and $NA_{DoS}$ for a subset of failed power lines varying the parameter $k_{PacksentRate}$*

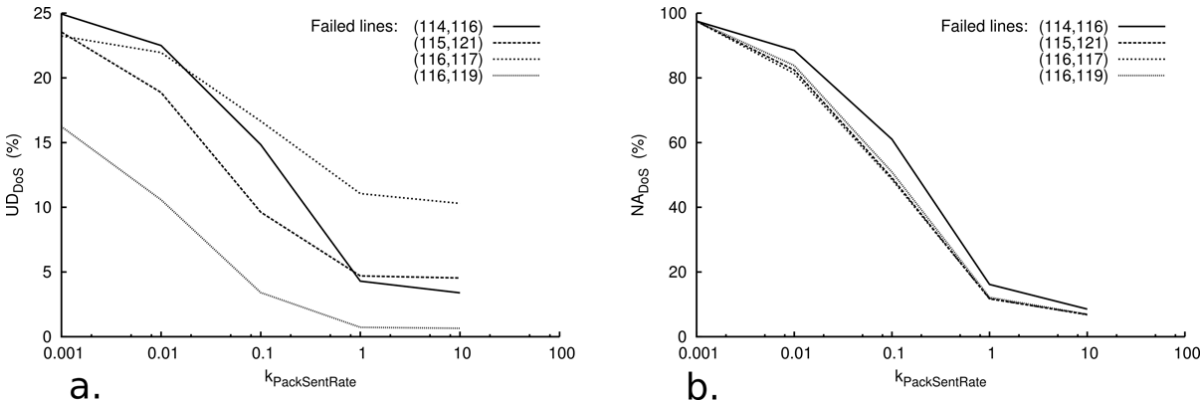
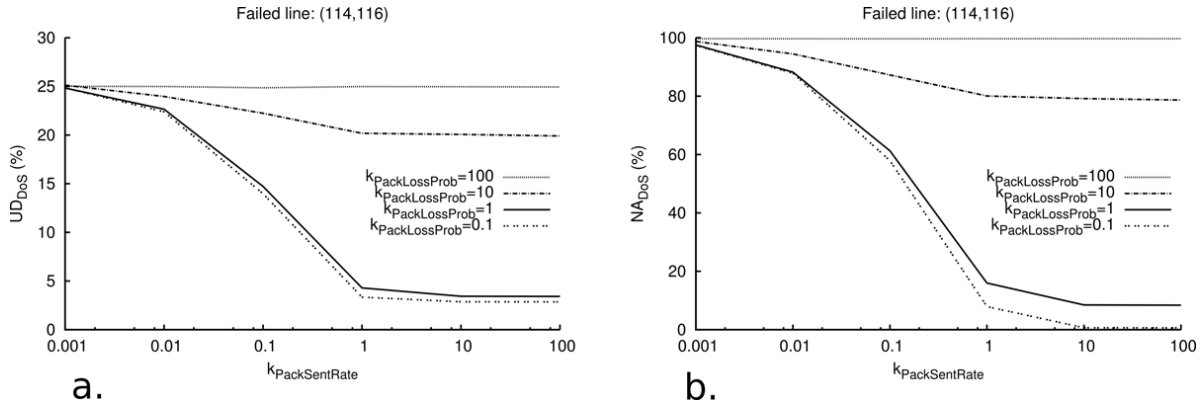



*Figure 8. $UD_{DoS}$ and $NA_{DoS}$ for the failed power line (114-116) varying the parameters $k_{PacksentRate}$ and $k_{PackLossProb}$*



40.000 batches, or of a number of batches adequate to reach a confidence level of 0.95.

Figure 6 shows the results of a first set of experiments, aimed at investigating how the severity of the DoS affecting the II infrastructure impacts on both the measures $UD_{DoS}$ (percentage of unsupplied load) in Figure 6a, and $NA_{DoS}$ (percentage of not armed substations), in Figure 6b, when individual power lines (as reported on the x-axis) fail. To improve readability, only a subset of the power lines are shown, selected among those that have a significant impact on $UD_{DoS}$.

The measure $UD_{DoS}$ has been evaluated for all the DoS behaviours considered in our study, while for $NA_{DoS}$ we limited the evaluation to increasing and decreasing severity behaviours (TDIS and TDDS) only, since the value of this measure is 100% or 0 for the two extreme DoS behaviours LCSU and LCSR (no LCS reachable and all LCS reachable), respectively.

For both measures, the impact of the DoS depends upon the failed line (the EI component) and ranges from a few percent to 25%, depending on the severity of the DoS attack (the II component). Focusing on $UD_{DoS}$, it can be noted that, not surpringly, the highest impact is shown by the worst DoS behaviour, that is when all LCS are not reachable. However, for almost half of the shown power lines this impact is rather low (below 3%).

Moving to $NA_{DoS}$ in Figure 6b, the effect of the decreasing severity behaviour of the DoS (TDDS) is significantly heavier than that of the opposite case of increasing severity (TDIS) on the percentage of not armed substations. Actually, for the TDIS behaviour, this percentage is rather low and remains almost constant for any of the failed power lines considered. In fact, the increasing DoS severity is better coped with, since the starting level of severity is low and, according to the parameters setting we selected, the reconfiguration performed by RS2() is possible within the time of increase of the severity level.

Finally, note that there is no direct relationship between the trend of the two measures: the percentage of not armed substations is significantly high for failed power lines in the right part of Figure 6b, while correspondingly the unsatisfied load is very low. Certainly, the linear programming problem at the basis of the reconfiguration solution computed by RS2() contributes to this effect, although further investigations would be desirable (and we are currently exploring other effects).

The TDDS DoS behaviour is the second most impacting after the extreme LCSU case, so it has been taken as the default DoS attack behaviour in our next set of analyses that concentrate on studying the effects on $UD_{DoS}$ and $NA_{DoS}$ on a subset of four power lines taken from those whose failure is particularly critical, as revealed by Figure 6a. Figure 7 shows the results of this analysis, again for both indicators under assessment, varying the rate at which the arming commands are transmitted by activity *Sent*. This rate is different for each severity level of the DoS, and to vary it consistently we have used a multiplicative factor, represented by the parameter $k_{PacksentRate}$ on the x-axis. This parameter ranges from $10^{-3}$ to $10^{2}$, so the packet sent rate varies in the analysis from 1/1000 to 100 times the default values reported in Table 1). The trend common to both measures is that, when the arming command is delayed with respect to the default value (portion of the figures at the left of $k_{PacksentRate}=1$), worse results are obtained, while almost no improvement is observed for lower delay (portion of the figures at the right of $k_{PacksentRate}=1$). Comparing it with Figure 6a, we observe that the arming delay resulting from $k_{PacksentRate}=0.001$ leads to the worst load loss for the power lines considered.

To investigate more deeply into the system behaviour we have performed another analysis, whose results are shown in Figure 8. This analysis concentrates on the system behaviour upon the failure of the power line with the highest impact on both $UD_{DoS}$ and $NA_{DoS}$, that is line (114,116), for different values of the probability of losing an arming command, under the default TDDS DoS severity. Also this probability is different for

each severity level of the DoS, and, similarly to the previous analysis, to vary it consistently, we have used a factor represented by the parameter $k_{PackLossProb}$ on the x-axis (which ranges from 0.1 to 100, but keeping the resulting probability value up to 1).

For both measures, it can be observed that, lowering the probability of losing an arming command with respect to the assumed default value does not bring benefits ($k_{PackLossProb}<1$). Instead, a significant worsening is obtained when this probability increases. The most interesting result from this analysis is the combined effect of the two parameters $k_{PackLossProb}$ and $k_{PackSentRate}$. Decreasing the delay in sending an arming command does not lead to relevant gain when the probability of losing the command is high (10 or 100 times the default value, in the figure). Instead, for values of $k_{PackLossProb}<=1$, decreasing the delay in sending an arming command (moving from $k_{PackSentRate}=0.01$) leads to significant improvements, until the best obtainable values for $UD_{DoS}$ (when $k_{PackSentRate}=1$) and $NA_{DoS}$ (when $k_{PackSentRate}=10$), corresponding to LCSR case (Figure 6).

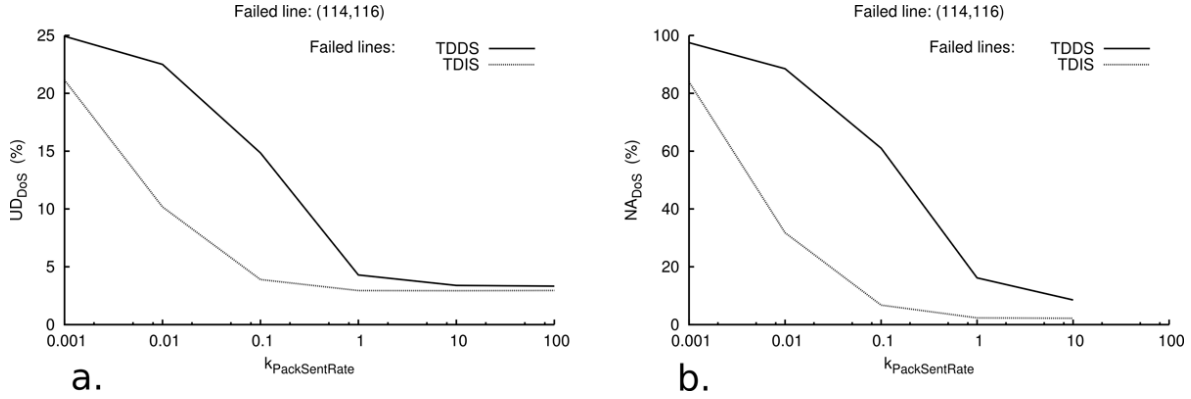
Finally, Figure 9 presents the results of $UD_{DoS}$ and $NA_{DoS}$, in presence of both TDDS and TDIS attack behaviours. It can be noted that worse values are shown in the case of TDDS, confirming the results of previous analyses. Interestingly, the highest difference between the curves in both Figures 9a and 9b occurs in correspondence of $k_{PackSentRate}=0.01$. Then, increasing the value of this parameter implies that the delay in sending the arming command decreases, weakening the difference in impact by the two DoS cases towards having TDDS having the same effect as TDIS, until the best values are reached by both $UD_{DoS}$ and $NA_{DoS}$. Instead, decreasing the value $k_{PackSentRate}$ below 0.01 results in the opposite effect, and it is TDIS that resembles the effects of TDDS, raising the values of both $UD_{DoS}$ and $NA_{DoS}$ until the worst values they can reach.

## FUTURE RESEARCH DIRECTIONS AND CONCLUSION

The presented framework can be adapted to model other types of cyber attack. For instance the DoS attack may affect the communication channel between the TSO sentinel and the DSO SSs that may cause both a premature disarming due to the delay/loss of some test packet and the delay/loss of the trip command.

In details this would require to explicitly model the communication channel between the TSO sentinel and the DSO SSs, besides the one

*Figure 9. $UD_{DoS}$ and $NA_{DoS}$ for the failed power line (114-116) for the two cases of increasing and decreasing severity*



between the DSO CC and the DSO SSs already included in the current model.

The same atomic model representing the communication network may be replicated to this purpose, however in the new scenario we should consider two types of messages modeling the test packet and the trip command. This can be avoided if the test packets are not explicitly modeled but their effect could be emulated by adding a (DoS severity level dependent) probability of shortening the disarming timeout. In the new scenario, the RS2 can fail when a set of armed DSO SSs have been disarmed due to the delay/loss of their test packets or when armed DSO SSs are excluded by the load shedding due to the delay/loss of their trip commands.

Intrusion attacks instead could be dealt with by embedding a new atomic model representing a possible set of attack scenarios with an incremental propagation of the intrusion attack towards the target node(s) of the II and possibly an incremental restoration of II nodes representing the successful application of an Intrusion Prevention System (IPS) protection strategy.

In this context, when target nodes are reached, a subset of DSO SSs becomes unreachable and cannot participate to the load shedding strategy.

This could be modeled exploiting the multi-formalism facilities of Möbius so that the attack propagation schema as well as the IPS countermeasure behaviors could be represented by means of a Fault Tree or their extensions (Codetta, Iacono, Franceschinis & Vittorini, 2004).

It has been the goal of this chapter to show how a model based approach can provide a way to reason about the possible consequences of vulnerabilities present in one infrastructure on the other, in particular we have studied the case of how a cyber attack can worsen the service provided by an Electrical Grid. An abstract but sufficiently precise description of both the electrical infrastructure operation and of the ICT control system procedures together with their interaction schemas allow to point out the influence that a failure in one subsystem may have on the other, with particular attention to the cascading or escalating effects.

This paper has concentrated on a quantification of the impact of a cyber attack in terms of two quantities. A more "customer oriented" measure (the percentage of undelivered load) and one which can be seen as more "grid management oriented" (the percentage of substations that are not able to participate in the load shedding activities due to a cyber attack).

A relevant issue for quantification is the choice of the parameters characterizing the times, the failure probabilities, and in general all the relevant quantitative characteristics influencing the final results: this opens many interesting considerations on the possible interactions with experimental settings: from the exchange of parameters, to the model validation, to the selection of the most interesting sets of experiments.

## REFERENCES

Baumeister, T. (2010). *Literature review on smart grid cyber security*. Technical Report. Retrieved from http://csdl.ics.hawaii.edu/Plone/news/news_item.2010-12-28.4892508419

Beccuti, M., Chiaradonna, S., Di Giandomenico, F., Donatelli, S., Dondossola, G., & Franceschinis, G. (2012). Quantification of dependencies between electrical and information infrastructures. *International Journal of Critical Infrastructure Protection*, *5*(1), 14–27. doi:10.1016/j.ijcip.2012.01.003

Beccuti, M., Franceschinis, G., Donatelli, S., Chiaradonna, S., Di Giandomenico, F., Lollini, P., et al. (2009). Quantification of dependencies in electrical and information infrastructures: The CRUTIAL approach. In *4th International Conference on Critical Infrastructures (CRIS 2009), Linkoping, Sweden,* (pp. 1-8). IEEE Computer Society Press.

Bloomfield, R., Buzna, L., Popov, P., Salako, K., & Wright, D. (2009). Stochastic modelling of the effects of interdependency between critical infrastructures. In E. Rome & R. Bloomfield (Eds.), *4th International Workshop on Critical Information Infrastructures Security (CRITIS 2009): LNCS Vol. 6027* (pp. 201-212). Berlin, Germany: Springer.

Bompard, E., Napoli, R., & Xue, F. (2009). Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection*, *2*(2), 5–12. doi:10.1016/j.ijcip.2009.02.002

Chiaradonna, S., Di Giandomenico, F., & Lollini, P. (2008). Evaluation of critical infrastructures: Challenges and viable approaches. [Springer Verlag.]. *Architecting Dependable Systems, LNCS*, *5135*, 52–77. doi:10.1007/978-3-540-85571-2_3

Chiaradonna, S., Di Giandomenico, F., & Lollini, P. (2011). Definition, implementation and application of a model-based framework for analyzing interdependencies in electric power systems. *International Journal of Critical Infrastructure Protection*, *4*(1), 24–40. doi:10.1016/j.ijcip.2011.03.001

Chiaradonna, S., Di Giandomenico, F., & Nostro, N. (2011). Modeling and analysis of the impact of failures in electric power systems organized in interconnected regions. In *41st International Conference on Dependable Systems & Networks (DSN2011)*, Hong Kong, China, (pp. 442-453). IEEE Computer Society Press.

Chiaradonna, S., Lollini, P., & Di Giandomenico, F. (2007). On a modeling framework for the analysis of interdependencies in electric power systems. In *IEEE/IFIP 37th International Conference on Dependable Systems and Networks (DSN2007)*, Edinburgh, UK, (pp. 185-195). IEEE Computer Society Press.

Codetta, R. D., Iacono, M., Franceschinis, G., & Vittorini, V. (2004). Repairable fault tree for the automatic evaluation of repair policies. In *International Conference on Dependable Systems and Networks (DSN2004),* Florence, Italy, (pp. 659-668). IEEE Computer Society Press.

Coppolino, L., D'Antonio, S., Elia, I. A., & Romano, L. (2011). Security analysis of smart grid data collection technologies. In F. Flammini, S. Bologna, & V. Vittorini (Eds.), *30th International Conference, SAFECOMP 2011, LNCS 6894* (pp. 143–156). Berlin, GermanyL Springer-Verlag Heidelberg.

CRUTIAL. (n.d.). *European Project CRUTIAL - Critical utility infrastructural resilience*. Retrieved from http://crutial.rse-web.it

Daly, D., Deavours, D. D., Doyle, J. M., Webster, P. G., & Sanders, W. H. (2000). Möbius: An Extensible Tool for Performance and Dependability Modeling. In B. R. Haverkort, H. C. Bohnenkamp, & C. U. Smith (Eds.), *11th International Conference, TOOLS 2000: LNCS Vol. 1786* (pp. 332-336). Springer Verlag.

Hahn, A., & Govindarasu, G. (2010). Smart grid cybersecurity exposure analysis and evaluation framework. In *IEEE Power and Energy Society General Meeting*, (pp. 1-6).

Hahn, A., & Govindarasu, M. (2011). Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, *2*(4), 835–843. doi:10.1109/TSG.2011.2163829

IEEE RTS Task Force of the APM Subcommittee. (1996). The IEEE reliability test system - 1996. *IEEE Transactions on Power Systems*, *14*(3), 1010–1020.

IRRIIS. (n.d.). *European Project IRRIIS - Integrated risk reduction of information-based infrastructure systems*. Retrieved from http://www.irriis.org/

Klein, R. (2008) Information modelling and simulation in large dependent critical infrastructures: An overview on the European integrated project IRRIIS. In R. Setola & S. Geretshuber (Eds.), *3rd International Workshop on Critical Information Infrastructures Security (CRITIS 2008): LNCS Vol. 5508* (pp. 131-143). Berlin, Germany: Springer.

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation*. Hoboken, NJ: Wiley & Sons Inc. doi:10.1002/0471789542

Lippman, R. P., & Ingols, K. W. (2005). *An annotated review of past papers on attack graphs. Project Report*. Lincoln Laboratory.

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, *7*(3), 75–77. doi:10.1109/MSP.2009.76

Nieuwenhuijs, A., Luiijf, E., & Klaver, M. (2009). Modeling dependencies in critical infrastructures. In Papa, M., & Shenoi, S. (Eds.), *International Federation for Information Processing (IFIP2009)* (*Vol. 290*, pp. 205–213). Boston, MA: Springer.

Romani, F., Chiaradonna, S., Di Giandomenico, F., & Simoncini, L. (2007). Simulation models and implementation of a simulator for the performability analysis of electric power systems considering interdependencies. In *10th IEEE High Assurance Systems Engineering Symposium (HASE2007),* Boca Raton, Florida, USA, (pp. 305-312). IEEE Computer Society Press.

Sanders, W. H. (2010). *Progress towards a resilient power grid infrastructure.* Paper presented at the meeting of IEEE Power & Energy Society General Meeting (PES GM), Minneapolis, Minnesota, USA.

TCIP-G project. (n.d.). *Trustworthy cyber infrastructure for the power grid.* Retrieved from http://tcipg.org/

Ten, C.-W., Liu, C.-C., & Govindarasu, M. (2007). *Vulnerability asessment of cybersecurity for SCADA systems using attack trees.* Paper presented at the meeting of IEEE Power Engineering Society General Meeting, 2007.