Quantification of Dependencies between Electrical and Information Infrastructures

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

Quantification of dependencies between electrical and information infrastructures

Marco Beccuti[a], *Silvano Chiaradonna*[c], *Felicita Di Giandomenico*[c], *Susanna Donatelli*[a,*], *Giovanna Dondossola*[d], *Giuliana Franceschinis*[b]

[a] *Dipartimento di Informatica, Univ. di Torino, Turin, Italy*
[b] *Dipartimento di Informatica, Univ. Piemonte Orientale, Alessandria, Italy*
[c] *Istituto ISTI, CNR, Pisa, Italy*
[d] *Dipartimento Sviluppo dei Sistemi Elettrici, RSE S.p.A., Milan, Italy*

ARTICLE INFO

Article history:
Received 4 October 2010
Received in revised form
17 November 2011
Accepted 20 January 2012
Published online 28 January 2012

Keywords:
Modeling
Electrical power system
ICT threats
Critical infrastructure dependencies

ABSTRACT

In this paper we present an approach to model and quantify (inter)dependencies between the Electrical Infrastructure (EI) and the Information Infrastructure (II) that implements the EI control and monitoring system. The quantification is achieved through the integration of two models: one that concentrates more on the structure of the power grid and its physical quantities and one that concentrates on the behavior of the control system supported by the II. The modeling approach is exemplified on a scenario whose goal is to study the effects of an II partial failure (a denial of service attack that compromises the communication network) on the remote control of the EI. The approach has been initially developed as part of the European project CRUTIAL.

1. Introduction

Electrical Power Systems (EPS) supply a vital oxygen to people lives. Ongoing infrastructural and organizational transformations in the energy sector have to guarantee the continuous availability of power provisions. There is evidence that EPS blackouts are often caused by a concurrency of events, that include classical physical faults in the electrical components, but also wrong or untimely behavior from the control systems and/or their human operators, often caused or exacerbated by a malfunctioning of the telecommunication system that supports the EPS control. EPS players are paying increasing attention to the possibility that such malfunctioning is actually caused by malicious threats to control systems, and special attention is devoted to understand the dependencies between the electrical grid, the control systems that manage the grid and the telecommunication networks that support the control.

In this paper we focus on the dependencies between the Information and Communication Technology (ICT) system (in particular the telecommunication component) and the electrical grid being controlled, in particular we investigate the consequences of a malfunctioning of the communication system when the grid has just experienced a failure, like the loss of a generator or the tripping of a line. This is a scenario in which a timely (remote) control action is vital to avoid a failure propagation that may potentially lead to large black-outs.

Considering the crucial role of control systems in governing the quality and the stability of the electric power service,

[*] *Corresponding author.*
E-mail address: susi@di.unito.it (S. Donatelli).

1874-5482/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2012.01.003

it is considered of great importance for the utilities operating the infrastructures to have tools for analyzing threat impacts and technologies for avoiding, or limiting, most serious consequences. In this paper the considered scenario is studied through modeling, due to its high flexibility in exploring a wide range of alternatives at a limited cost. In particular a stochastic modeling approach has been pursued allowing us to represent randomness of physical faults and to model at a sufficiently high abstraction level the effect of malicious attacks as they propagate under variable network conditions.

These studies have been pursued in the framework of the EU project CRUTIAL [1], that has developed an architectural framework to improve the resiliency of power control systems in the presence of threats to their information and communication infrastructures. The project focused on the electrical and the information infrastructures (EI and II), by considering different topologies and different kinds of risk, identified through a set of *scenarios* that illustrate interesting patterns of interaction between the EI and the II.

In order to master the complex mechanisms of global failures, particular focus was put on the study and modeling of the types of failures that are characteristic of interdependent critical infrastructures. Although the modeling of such failures has received increasing interest in the last years after the large blackouts of electric power transmission systems in 1996 and 2003, there is still no definite understanding on EPS interdependencies, and on the techniques to evaluate the impact of cascading, escalating and common cause failures.

The modeling framework developed in CRUTIAL includes both qualitative and quantitative models. Qualitative models are aimed at capturing the interaction between EI and II [2] and have led to the definition of a new class of automata [3]. Qualitative modeling will not be discussed in this paper, that concentrates instead on *quantitative modeling*.

This paper summarizes the two different quantitative approaches that have been pursued and proposes a way to integrate the two to get a more faithful description of the EI, the II and the impact that a malicious attack on the latter has on the former, in particular when facing a critical scenario.

The first approach, described in Section 4, is based on Stochastic Well-formed Nets (SWN) [4,5] and is more centered around the protocols addressed by the scenario and a Denial of Service (DoS) attack, while the EI behavior is described in very abstract terms. A preliminary version of this model was described in [6].

The second approach, described in Section 5, is based on an integration of a Stochastic Activity Network (SAN) [7,8] model of the EPS with techniques imported from the power engineering field to model and simulate the electrical state of the EPS. A preliminary version of this model has been described in [9,10]. This approach (that we shall call SAN for short) allows a rather detailed model of the EPS; however the model of the control algorithms and of the counter measures that take place upon a failure are treated at a rather abstract level.

In these two sections the SWN and SAN models are revisited so as to pave the way for the integration of the two, described in Section 6: it is by integrating the two models that we reach an adequate level of detail in both the EI and II behavior and shed some light on the interplay between the two infrastructures. The quantitative analysis of the integrated model allows us to stochastically quantify the effects of the dependencies between EI and II when a cyber threat is in action: the integration is cast in the context of a failure scenario in which a DoS attack disrupts the communication abilities of the EPS control centers. The scenario is described in Section 3.

Section 7 reports an extensive analysis of an example grid, under the target scenario, to enlighten the different types of analysis that can be performed using the integrated model.

Conclusions are finally drawn in Section 8.

This paper is an extended version of the preliminary work presented at the CRIS conference [11]. In this extended version the various forms of model interactions have been clarified and extensive experimental results have been added.

2. Previous literature

Understanding the reciprocal effects of interdependencies among interacting critical infrastructures (CI), as well as quantifying resiliency, security and robustness related indicators are tackled by a number of research initiatives/organizations. An overview is provided in [12]. A rigorous approach to analyze and understand how infrastructure sectors (including water, power, energy, telecommunications, and the Internet) evolve, where they are vulnerable, and how they can best be protected is presented in [13].

The European project IRRIIS [14] devoted significant effort to interdependency analysis and modeling, with special focus on scenarios describing the future situation with respect to telecommunication and electricity infrastructures in 2015. A theoretical framework has been developed in [15], where an approach equivalent to process modeling is adopted, which views a CI as a process and dependencies are modeled as response functions. Quantitative interdependency analysis, in the context of Large Complex CI, is presented in [16], where a discrete state–space, continuous-time stochastic process models the operation of critical infrastructures, taking interdependencies into account. Of primary interest are the implications of both the level of model abstraction and model parametrization for the study of dependencies on the distribution of cascade-sizes within and across infrastructures. Also, the Leontief input–output economical model dedicated to the market dynamics representation has been exploited and adapted to model critical infrastructures dependencies. Recently, in the context of the EU MIA (Methodology for Interdependencies Assessment) project, a Markov Chain law replaces the Leontief equilibrium condition upon external changes, thus allowing us to follow the transition from one equilibrium configuration to another and possibly mimic cascade effects triggered by unwilled disturbances [17]. Among the empirical studies, in [18] an empirical approach is applied to analyze a large set of CI failure data, to discover patterns across infrastructure failures. The IRRIIS consortium has also developed SimCIP (Simulation for CI Protection), an agent-based simulation environment for controlled experimentation, intended to be used to deepen the understanding of critical infrastructures and their interdependencies [19]. The power blackout scenario, taken as a reference scenario for SimCIP, focuses on the dependencies of the telecommunication infrastructure from the power supply. Our framework is based on stochastic models, similar to [16], but it is specifically tailored to EPS and allows us to deal with a more detailed representation of the major components and dynamics of the electric grid and related ICT control. In terms of evaluations of power versus ICT interdependencies, the IRRIIS scenarios are complementary to those illustrated here.

Several other models based on simulation have been proposed to accomplish interdependencies analysis, especially with reference to EPS alone [20,21] and in connection with telecommunication networks [22–25]. These studies mainly focus on reproducing network disruptions, which eventually lead to blackouts, in order to estimate the vulnerabilities of the system or the impact on the EPS reliability of important network parameters. However, most of the existing models do not provide explicit modeling of the main interdependent subsystems and of the interdependencies between such subsystems, so evaluation of the impact on dependability and performability of cascading or escalating failures is not trivial. Only in [21], interactions between EI disturbances and the often imperfect human operator control actions have been considered.

The National Science Foundation project TCIP, currently extended in TCIP-G with support also from the Department of Energy and contributions from the Department of Homeland Security, focuses on securing 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 [26], 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. A variety of evaluation tools are adopted to enable validation, including PowerWorld, RINSE, formal logic, PowerWeb and APT. 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.

Several other works have been directed to analyze structural vulnerabilities and the risk of cyber attacks. In [27], 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 (e.g., degrees of nodes and global efficiency) with two new metrics, entropic degree and netability, accounting for the physical/operational behavior of power grids in terms of real power-flow allocation over lines and line flow limits. 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. In the research activity by Liu et al. [28] the risk of cyber attacks on the power system is calculated as the product of two factors: the probability of a successful intrusion and the impact of the intrusion as unserved load. The two risk factors are evaluated by two separate techniques. The cyber layer underlying substation control systems is analyzed through stochastic firewall and password models, while the impact factor for the attack upon a Supervisory Control And Data Acquisition (SCADA) system is measured by the ratio loss of load/total load through power flow simulation. Experiments are conducted on a case study via simulation of the power flow and dynamic analysis. The possibility of integration of the cyber and power models is based on the simplifying assumption that cyber attacks provoke the unexpected opening of circuit breakers and, consequently, the correspondent loss of load. However, in these studies interdependencies aspects are not dealt with specifically.

More recently, the issue of how to measure the level of interdependencies and to identify appropriate metrics for quantifying their strength is being addressed in a few studies, such as [29–31]. These studies are orthogonal to our objective and could be profitably employed to guide the analysis of EPS by concentrating on those interdependencies showing an higher degree of strength.

3. The reference scenario and analysis objectives

The model interaction presented in this paper is applied to the telecontrol scenario developed in CRUTIAL [32], and shows the interaction between II and EI in presence of DoS and electrical failures. It involves both Transmission and Distribution System Operators (TSO and DSO respectively), but it only considers the DoS attack affecting the DSO net. 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 more severe damages to the EI.

Let us explain such a scenario in more detail and introduce the main TSO and DSO operators involved. In emergency conditions the TSO is authorized by the DSO to activate load shedding activities on the distribution grid; therefore the **TSO Control Center (CC)** monitors the Electric Power System and detects some potentially dangerous conditions that could be recovered with appropriate load shedding commands applied to particular areas of the grid. In order to actuate this defense/recover action the TSO CC chooses a subset of **DSO Substations (SSs)** from the list of DSO SSs participating in the emergency plan, then it sends the requests of preventively arming the control units of these DSO SSs to their **DSO Control Centers (CCs)**. These requests are delivered from the TSO CC to the DSO CC through a shared communication channel. Then the DSO CC forwards the arm command to the required DSO SSs, and returns their status to the TSO CC.

At the same time, a special TSO node called the **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 a real emergency situation is detected the TSO sentinel sends the load shedding action 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 the expected test packet within 1 min, it automatically disarms itself. Disarming also occurs after 20 min from the arming command if no load shedding command is issued by the sentinel.

In this context different behaviors can be envisaged depending on *when* the DoS occurs. For instance, a DoS attack starting before issuing the arming command towards a given DSO SS creates the possibility of preventing the execution of that DSO SS trip command. Instead, if a DoS attack takes place when the substation is armed, the attack may deny the successful execution of the periodic testing and causes the consequent automatic disarming of all/some DSO SSs. Finally, the DoS may occur just before sending the load shedding command thus denying the possibility of defending the system from extreme contingencies.

Therefore the effects of the considered DoS on the EPS will depend on the number and position of DSO SSs affected by the attack and on the pattern and intensity of the DoS.

The identification of the dependencies of EI and II upon an electrical failure in presence of a DoS, and their quantification, is the aim of the work presented in this paper.

4. The SWN model

The ICT control system implemented by the II infrastructure is modeled using SWN [5]: an high level Stochastic Petri Net formalism, where tokens may have identities (colors), and transitions may fire either immediately or after a random delay characterized by a negative exponential distribution. Hereafter we assume that the reader is familiar with SWNs, a complete description of this formalism can be found in [5].

The SWN model is shown in Fig. 1(A), where its submodels, highlighted by dotted boxes, correspond to the components described in the previous section (i.e. TSO CC, DSO CC, communication channel, DSO SS, TSO sentinel, EI and Attacker submodels). It is a refinement of the one presented in [6].

It details the flow of events of the load shedding process among the TSO CC, the DSO CC, the DSO SSs, and the TSO sentinel, while the status of the EI and the attack is modeled as an external environment (Attacker and EI submodels). We do not explicitly model the causes of a failure in EI, of an arming by the TSO CC or of an attack to the communication, but we consider each of them as regulated by a stochastic law expressed by transitions *e-failure* and *e-failure1* in the EI submodel, *StartArmingProcess* and *EndArmingProcess* in the TSO CC submodel, and *Begin_attack*, *End_attack* in the Attacker one.

The TSO CC submodel interacts with the rest of the model through transition *TransmitArming*, that sends the arming commands to the DSO CC.

The EI submodel interacts instead through its state: when it is in Partial outage the TSO sentinel issues a load shedding command (transition *LoadShedding*), while a successful completion of the load shedding causes an *e-restoration* which takes the EI back to the state *e-working*. If the transition *e-restoration* does not fire before the occurrence of a second *e-failure* then the EI state becomes *e-lost* and the transition *#Reset* fires. Note that transition *#Reset* is equipped with a special semantics: when it fires it brings the model back to the initial marking.

In the model we assume a discrete number of DoS severity levels (*L*1 to *L*4) modeled by the colored class *C*2. When place *Active* is marked, transition *IncreaseSeverity* increases the severity level (*AttackSeverity* place). Instead when the attack is over, the place *Idle* is marked and transition *e-restoration* takes the severity level back to *L*1. The attacker submodel influences the transmissions from DSO CC to DSO SS (DSOtoSS-COM submodel) and back (SStoDSO-COM): transitions rates are defined so that a higher severity of the attack makes more probable to lose or delay packets (*LostPacket* and *TxDelay* transition weights depend on the marking of the *AttackSeverity* place).

In the addressed scenario TSO arms a subset of DSO SSs, and the precise subset depends on the arming policy. Substations are identified by colors of the class C1, and *z* commands are generated for *z* different DSO SSs colors (transitions *CC_selection*, *CC_endselection* and associated places). The DSO CC submodel also includes the reception of an acknowledge from the substations (places *DSO_CC_buffer_in*, *Commands* and associated transitions), which allows the DSO to detect an anomaly if an acknowledge is not received for too long (place *Packet_loss* and associated transitions). When an arming command is received by the DSO SS, the substation executes the arming (transition *Exec*), sets its state to armed (token in place *SS_armed*), and sends back an acknowledge that, as the arming command itself, can be lost or delayed depending on the presence and severity of an attack. According to the scenario a substation stays armed for at most 20 min, after which a disarming occurs (transition *ArmedExpired*). Observe that this model does not consider the DSO SS disarming when no test packets are received.

The last submodel is for the TSO sentinel, that issues a load shedding command to all DSO SSs (place *LSpending*). Since only armed substations can execute a load shedding, and since not all arming commands may have been received in time or received at all, the e-restoration may end successfully (transition *e-restoration* enabled when at least *k* DSO SSs were armed) or not (transition *Fail_e-restoration*).

The model is parametric in the number of substations (cardinality of the color class C1), in the number of levels of DoS (cardinality of the color class C2), in the number *z* of DSO SSs chosen by the arming policy, and in the minimum number *k* of substations that need to successfully complete a load shedding for the e-restoration to take place. It is also parametric on all stochastic elements (delays and probabilities of choices). Additional flexibility is allowed also by the modular construction, which allows us to plug-in other models of DoS or other types of attacks, as long as they interact by influencing the transmission of packets (loss probability and transmission delay).

The scope and the assumptions behind this model and its placement with respect to our analysis objectives will be discussed in Section 6, where its integration with the SAN

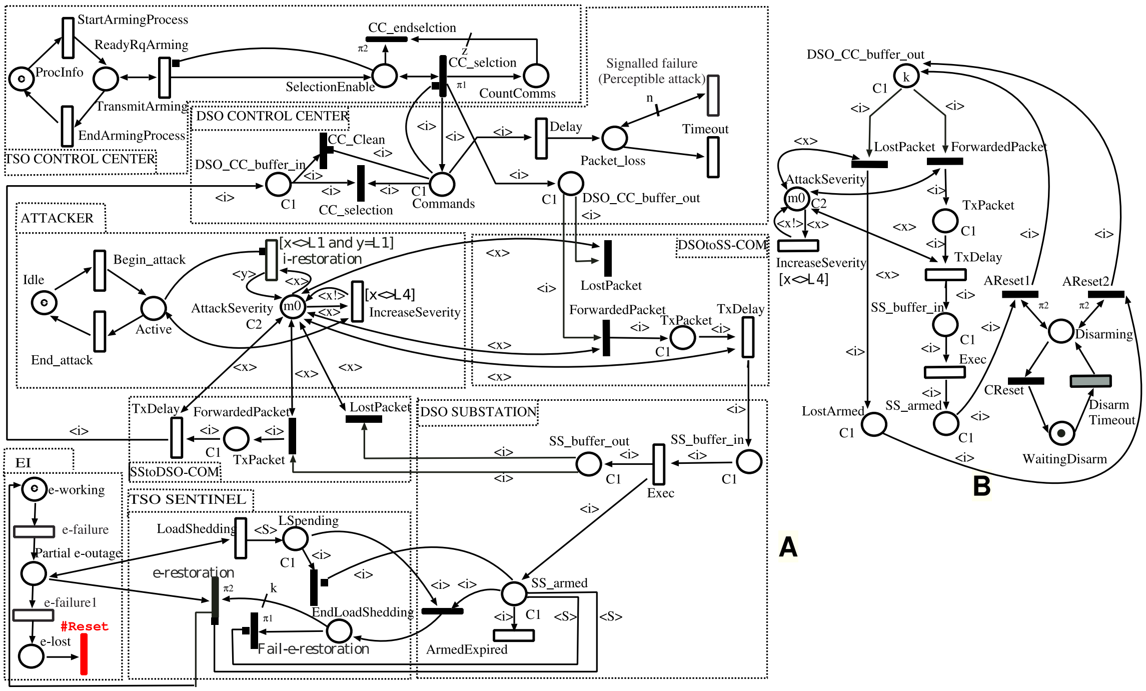

Fig. 1 – (A) SWN model of the DoS scenario; (B) simplified SWN for the interaction with the SAN model.

model is also proposed. In Section 6 we shall also discuss the possibility to further simplify this model (leading to the SWN in Fig. 1(B)) in the context of its integration with the SAN.

5. The SAN model

To allow a realistic estimation of the impact of the DoS on the EI, we have decided to make use of the SAN modeling approach of CRUTIAL, reported in [9,10,33], and here summarized in its general aspects and in those aspects that will be the base for the integration. The SAN approach has been developed in the context of the transmission grid and uses a terminology that is slightly different from the one used for the scenario and SWN description. However, it adapts to the distribution grid as well, since the electrical elements are the same and the II operations are abstracted in a way that can be easily extended for including the defense procedure of the reference scenario that requires communications among the distribution grid control components. To allow the reader to refer to both the original paper [9] and the scenario definition, we shall provide a mapping of the major terminology items.

Logical scheme of EPS. In the bottom part of Fig. 2, which depicts the logical structure of a homogeneous region of the transmission grid, we can see the main elements that constitute the electric infrastructure: *generators* (N_G components), *substations* (N_S components), *loads* (N_L components) and *power lines* (A_L components, which also logically include breakers and protections connected to the power lines).

In the upper part of Fig. 2 we have depicted a possible logical structure of a regional II, i.e., the part of the information system controlling and operating on a region of the transmission grid. The components *LCS* (Local Control System) and *RTS* (Regional Telecontrol System) differ for their criticality and for the locality of their decisions, and they can exchange grid status information and control data over a (public or private) network (*ComNet* component). *LCS* guarantees the correct operation of a node equipment and reconfigures the node in case of breakdown of some apparatus. *RTS* monitors its assigned region in order to diagnose faults on the power lines. In case of breakdowns, it chooses the most suitable corrective actions to restore the functionality of the grid. *RTS* corresponds to the TSO CC of the scenario, and *LCS* corresponds to the control units local to the TSO Sentinel (N_S components) and the DSO SS (N_L components) MCD-TU. Since in this scenario we assume a MCD-TU for each substation then *LCS* corresponds also to a DSO SS. Note that the concept of DSO control center is not explicitly modeled, but it is taken into account by the control function explained in the sequel (RS_1 and RS_2).

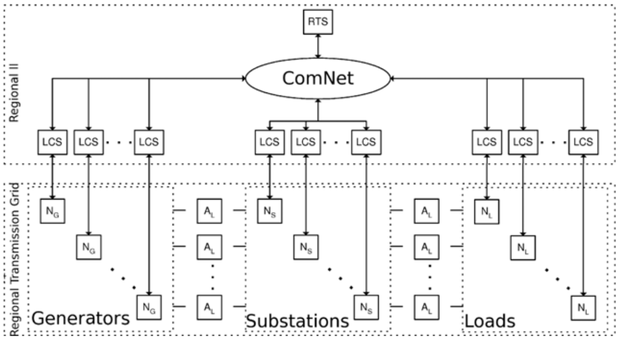

Fig. 2 – Logical structure of the analyzed EPS instance.

The operations performed by II are not considered in detail but they are abstracted at two levels, on the basis of the locality of the EI state considered by II to decide on proper reactions to disruptions. Each level is characterized by an activation condition (that specifies the events that 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: $RS_1()$, to represent the effect on the regional transmission grid of the reactions of II to an event that has compromised the electrical equilibrium[1] of EI, when only the state local to the affected EI components is considered. $RS_1()$ is performed by *LCS* components and, because of the limited information necessary to issue its output, it is fast in providing its reaction. $RS_2()$ is performed by RTS, 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, $RS_2()$ is determined on the global EI state and reacts in a longer time.

In the current implementation, the output of $RS_1()$ is obtained by the solution of power flow equations while minimizing a simple cost function, indicating the cost incurred in having loads not satisfied and having the generators producing more power. The output values of $RS_2()$ are derived by solving an optimization problem to minimize the change in generation or load shedding, under additional system constraints, as described in [34]. The reconfiguration strategy $RS_1()$ is applied immediately, while $RS_2()$ is applied after a time needed by *RTS* to evaluate it. All these functions are based on the state of EI at the time immediately after the occurrence of the failure.

SAN model of EPS. The logical EPS scheme just presented has been modeled through the SAN formalism [8] a generalization of Stochastic Petri Nets featuring state variables of any type (including doubles) and C-like functions to express transition enabling and state change. The models have been simulated through Möbius [7], a powerful multi-formalism/ multi-solution tool.

Several atomic models have been identified as building blocks to generate the overall EPS model, which are composed and replicated to obtain the full model of the EPS region.

The atomic models interact with each other by exploiting the feature of shared places of the SAN formalism. In the developed EPS model, shared places represent part of the states of the EPS, like the initial and the current power flow through each line of the grid, the status of the propagation of a failure or a lightning, the disrupted/failed components, the open lines, etc. Through these interactions, it is also possible to represent the interdependencies between II and EI subsystems and the subsequent cascading or escalation failures caused by malfunctions (either at cyber or electrical levels).

The developed SAN model supports the evaluation, through simulation, of performability measures [35], accounting for both dependability and performance of the analyzed infrastructures. Measures are defined through a reward structure that associates proper costs/benefits to generators/loads and interruption of service supply. In this paper, we concentrate on the expected percentage of undelivered power demand.

We shall discuss the scope and the underlying assumption of this model with respect to our analysis objectives more extensively in the next section.

6. Model interaction

While the SAN and the SWN models in isolation can be considered as models of the behavior of an EPS whose communication infrastructure has been attacked by a DoS, it is quite clear that there are a number of simplifying hypotheses behind it and that each of them represents more faithfully a specific point of view abstracting out other details. The SWN model assumes that the load shedding command is issued whenever the EI is in a *Partial e-outage* state, but this is not always the case in reality, it depends on the complete state of the EI. Similarly, the model assumes that the *e-restoration* can take place or not depending on the number of detached substations, and that any restoration is successful: again this depends on the state of the power grid, that is not included in the model. Nevertheless the modeling of the arming requests and successive load shedding command by the sentinel, in presence of a DoS, represents quite faithfully the scenario's behavior.

For what concerns the SAN model there are also a number of discrepancies with respect to the considered scenario. The control is a two-level hierarchy, while it is three levels (TSO-CC, DSO-CC and SS) in the scenario. Nevertheless some of this information is taken into account implicitly by the reconfiguration functions $RS_1()$ and $RS_2()$, for example the reconfiguration can be computed on a limited portion of the grid, thus "emulating" the subset of SS involved in an emergency plan as determined by the TSO-CC. The SAN model that has been presented in Section 5 can account for the loss of an electrical component, which is what triggers the computation of a new configuration of the electrical state of the grid. The SAN model can also account for a failure in the II, such as the DoS attack considered in the scenario, by modeling them in terms of the number of LCS components available for a reconfiguration. In the SAN model this number is computed based on a probability (constant in time) of an LCS being reachable or not. This is actually a weak point of this approach, since using a fixed probability does not model correctly an important characteristics of the DoS which is its inherently dynamic nature, so that its impact (in particular on the number of reachable LCS) changes over time, and this should be taken into account in the model.

To exploit the specific feature of each model, we have defined a method to integrate the results obtained by each of them.

Fig. 3 depicts the behavior of the EI and II upon EI-failures (left) and the behavior of the DoS attack in terms of its severity

[1] Events that impact on the electrical equilibrium are typically an EI component's failure or the insertion of a new/repaired EI component; for simplicity, in the following we will refer only to failures.

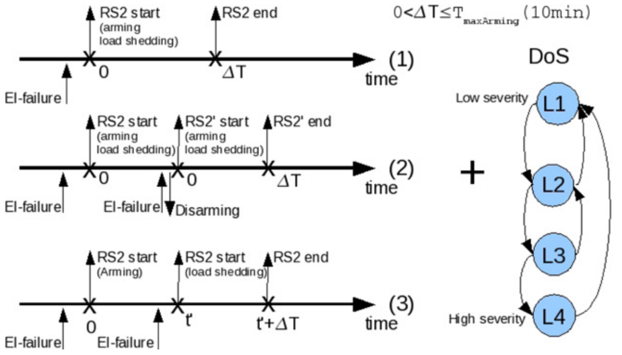

Fig. 3 – Timed evolution of the EI and II upon EI-failure and the DoS attack behavior.

levels (right): when an event occurs in the time-line, the result will depend on the severity level reached by the DoS attack at that point in time.

The first time-line of Fig. 3 depicts a case in which an EI-failure causes the start of the computation of $RS_2()$ at time 0. At time ΔT the computation terminates, the new configuration computed through $RS_2()$ is applied. If the reconfiguration was adequate a stable state is reached, if not, some electrical components will disconnect due to the local protections and a new $RS_2()$ is computed, leading potentially to a load shedding request. Observe that the reconfiguration success depends also on the DoS attack severity.

The second time-line shows a case, in which between time 0 and ΔT a second EI failure takes place. In this case the $RS_2()$ function is aborted, all the armed LCSs are disarmed, and a new $RS_2()$ function is started.

The third time-line shows a case where a low severity EI-failure happens followed by a high severity one: the former EI-failure moves the system in alert state and triggers the arming process at time 0, while the latter one moves the system in the alarm state and triggers the load shedding process at time t'.

The interaction between SWN and SAN takes place precisely on *the computation of the number of reachable and armed LCSs at time t given the arming process started at time* 0*, and given an initial DoS severity level*. This number is a random variable whose value at time t is distributed according to $prob(NumStation, t|InitDosLevel)$. This distribution is computed in isolation on the SWN as the number of armed substations at a finite time horizon t and for an initial DoS severity level. If we consider a behavior like that depicted in the first two time-lines of Fig. 3, and we consider that the DoS level at time 0 is L, then the SWN should compute the distributions at time ΔT given the initial DoS severity level L ($prob(*, \Delta T|L)$). Instead, if we consider the policy depicted in the last time-line, we should compute the distributions at times $t + \Delta T$ given the initial DoS severity level L ($prob(*, t + \Delta T|L)$). This is due to the fact that the arming process is triggered by the first EI-failure, while the load shedding process caused by the second EI-failure happens at time t. This approach requires a discretization of time with an appropriate time step, and the computation at each step the distribution of the number of reachable LCSs at time t (with t upper bounded by ΔT).

To compute the required distributions the SWN model can be significantly simplified (as depicted in Fig. 1(B)), since all the aspects concerning the Electrical behavior (issue of arming and load shedding commands, electrical failure, etc.) are already taken into account by the SAN model. The simplified SWN model can be considered as equivalent to the SWN model of Fig. 1(A) *conditioned* on the fact that an arming has been issued and that an attack has started. The simplified model includes the buffer where the arming commands are waiting to be transmitted from the DSO CC to the substations (place *DSO_CC_buffer_out*), along the way they can be lost (transition *LostPacket*) or delayed (transition sequence *ForwardedPacket*,*TxDelay*) due to the DoS attack effect; when a message reaches a substation input buffer (token in place *SS_buffer_in*) it eventually causes the arming of such a station (token in place *SS_armed*). Two additional submodels are included: one is used to update continuously the severity of the DoS attack (place *AttackSeverity* and transition *IncreaseSeverity*), while the other one models a timeout (Transition *DisarmTimeout*), after which the armed substations are disarmed and the behavior repeats again (possibly with a different DoS severity level). All the transitions except *DisarmTimeout* fire according to an exponential distribution. Transition *DisarmTimeout* is depicted in gray to emphasize that its firing time should be deterministic. In the experiments the deterministic has been approximated, to limit the solution cost, as an Erlang-3, modeled by a sequence of exponential transitions. From this model the probability distribution of the number of armed substations at time t, given an initial DOS severity level, can be computed.

These distributions can be used in the SAN model in two different ways. The first way consists of establishing the number of available LCSs, and then computing $RS_2()$ reconfiguration based on the estimated number k of available LCSs. The second way consists of applying $RS_2()$ on a predefined number of substations, but then only the actually reachable LCSs (according to the SWN model) are used to reconfigure the system. In the first case, $RS_2()$ reconfiguration is computed on k LCSs, then we use $prob(k, \Delta T|L)$ to decide if the reconfiguration induced by $RS_2()$ leads the EI in a stable state. In the second case, $RS_2()$ reconfiguration is still computed on k LCSs, but we use $prob(*, \Delta T|L)$ to compute the number of reachable LCSs at time t that will be really involved in the reconfiguration given the initial DoS severity level L.

7. Experimental results

To discuss the impact of dependencies between II and EI in presence of failures affecting both infrastructures, we have performed a set of experiments using the SAN and SWN models, for varying sets of parameters, but keeping fixed the grid topology.

7.1. EI grid

The analyzed grid is the “IEEE One Area RTS-96” of the IEEE Reliability Test System published in 1999 (RTS96)[2] [36],

[2] www.ee.washington.edu/research/pstca/rts/pg_tcarts.htm.

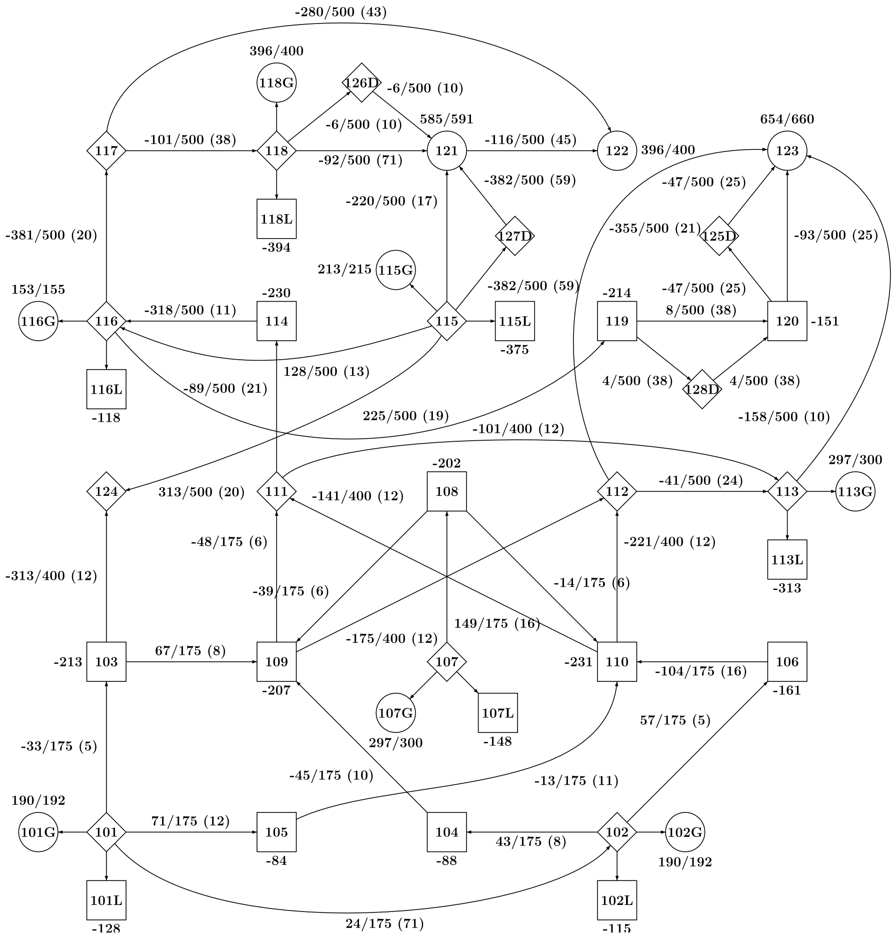

Fig. 4 – Diagram of the EI grid (generators are circles, loads are squares and substations are diamonds).

which has been frequently used in the past as a test power grid. The diagram shown in Fig. 4 is an abstraction of the topology "IEEE One Area RTS-96", where generators are circles, loads are squares and substations are diamonds. In the abstraction certain transformation in the description of the grid have been introduced. Since the SAN model does not explicitly model buses, the following transformations have been introduced: if there is a single load/generator on a bus, then only the load/generator is included in the model; if there is a load *and* a generator on the same bus *i*, this is modeled by a separate load *i*, a generator *i*, and a substation *i*, connected by dummy lines (lines for which a failure never occurs). A postfix *L* and *G* is added to load and generator identities *i* to provide a unique identifier. Another transformation has been introduced to ease the definition and solution of the linear programming problem which is part of the proposed evaluation process: each redundant line in the grid between any two nodes is replaced by two lines and a dummy substation (in Fig. 4 they are labeled 125D, . . . , 128D), and one of the lines and the substation cannot fail.

The label "P_i/P_i^{max}" associated with the generators represents the initial (active) power and the maximum power that a generator can supply. Note that in the grid we considered all the ratios P_i/P_i^{max} equal to the fixed value 0.99. The label "D_i" associated with the loads represents the power demand of a load. The label "F_{ij}/F_{ij}^{max} (b_{ij})" associated with each line represents the initial power flow through the line (F_{ij}), the maximum power flow that the line can carry (F_{ij}^{max}) and the susceptance (b_{ij}) used to determine the values for the power flow through the lines. For the sake of clarity, only the integer part of the original values associated to generators, power lines and loads are shown (in MegaWatt).

7.2. *Measures of interest*

The measures computed are defined in Table 1 and explained hereafter. Since the EPS is modeled as a stochastic process, the electrical energy provided to the final users (load ith) P_i and the electrical energy required by the final users (demand ith) D_i are random variables. Therefore, all the measures of interest we consider are the mean of random variables defined as a functions of P_i and D_i. The main measure of interest we consider is *UD*, defined as the percentage of the power demand that, on average, is not met in the interval $[0, t]$ (*UD* stands for "Unsatisfied Demand"). *UD* is a measure of the blackout size, defined as the mean of the load shedding 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 model

Table 1 – Definition of the performance indices.

Name	Definition
UD	$E\left[\frac{\sum_i \Delta P_i}{\sum_i \Phi_i}\right]$
UD_i	$E\left[\frac{\Delta P_i}{\Phi_i}\right]$
$PofUD_i$	$E\left[\frac{\Delta P_i}{\sum_i \Delta P_i}\right]$
nlUDgtK	$E\left[\frac{\sum_i \mathbf{1}\left(\frac{\Delta P_i}{\Phi_i} > \frac{k}{100}\right)}{nl}\right]$
ΔP_i	$\int_0^t (D_i(u) - P_i(u))du$
Φ_i	$\int_0^t D_i(u)du$
nl	Number of loads

enriched through the interaction with the SWN one, as explained in Section 6. For the computation we have used the simulator provided by the Möbius tool [7].

To gain a better insight, three additional measures have been defined. The measure *UD* can be computed "load by load", to provide an indication of the satisfaction of the single users connected to that load, leading to UD_i: the expected percentage of unsatisfied load collected "by load" *i*. To identify the most relevant loss, the measure $PofUD_i$ (percentage of unsatisfied load) has been introduced: it is defined as the expected percentage of power demand that is not met for each load *i* with respect to the total undelivered load. $PofUD_i$ can be seen as an indicator of how each load *contributes* to the unsatisfied demand. Finally, *nlUDgtK* allows to investigate the percentage of unsatisfied users, since it is defined as the expected percentage of the *nl* loads that have experimented a load loss greater than the *k*% of their demand.

All simulations reported have run with a relative accuracy of 0.1 and a confidence level of 0.95.

7.3. Parameters and failures considered

Each experiment performed includes the definition of the following aspects: power grid (topology, electrical parameters, and demanded load characteristics), EI failure and repair characteristics, II failure and repair characteristics, EI-II interaction. We shall take them one by one. A list of acronyms and parameters, including definitions and default parameters values, is shown in Table 2.

Grid. The reference grid introduced above has been used for *all* experiments. The load demand does not change over time, and the value of each load is indicated in Fig. 4.

EI failure and repair. At time zero, one power line is affected by a permanent disruption (generated by an external event, such as a tree fall or a terrorist attack), that makes it unavailable. The repair time of the failed power lines varies from 10 to 768 h (32 days), depending on the line. The parameters of the power grid control system have been fixed for all experiments reported here and they include the structure of the control (which nodes are controlled by which LCS), the time for the local reconfiguration $RS_1()$, which is considered negligible, and the time for a global reconfiguration $RS_2()$, which has been taken equal to 10 min (this specific value has been chosen taking into account the standard settings of power grids, in particular of the Italian one)

Although all experiments were performed assuming exactly one *external* EI failure, this does not mean that during the interval $[0, t]$ considered only one line can fail. Indeed this is in general *not the case*, since the SAN model includes failure propagation, that usually results in more power line failures, in load shedding actions, etc.

II failure and repair. The II failures considered are due to DoS attacks to communication channels between the DSO CC and the DSO SSs, as depicted by the SWN models. An SWN model of a DoS attack is characterized by the duration of the attack, the initial severity of the attack, the speed at which the severity of the attack increases, the probability to lose a packet and the average delay of a packet associated with each severity level of the attack. In all experiments the duration of the attack is exponentially distributed with mean equal to 24 h (the same expected value as for the duration of the EI line failure), which sets our experiments in the worst case scenario. The initial severity is instead a model parameter, while the rate at which the severity increases has been set to the fixed value of 8.3×10^{-3} min^{-1} (this value has been computed considering that the mean value of the distribution of the random variable "DoS duration" is 24 h). The settings of the probability of losing a packet (depending on the DoS attack severity levels) and of the rate of transition *TxDelay*

Table 2 – Acronym definition, parameters and their default values.

	Acronyms	
LCSU	All LCS unreachable	
LCSR	All LCS reachable	
FS	Fixed severity	
PIS	Probabilistically increasing severity	
TDS	Time dependent severity	
	SAN and SWN parameters	
	Repair time of the failed power lines	$10h, \ldots, 32d$
	Time for reconfiguration $RS\_2()$	10 min
	Duration of the DoS attack	24 h
w(IncreaseSeverity)	Rate at which the severity of the DoS attack increases	$8.3 \cdot 10^{-3}$ min^{-1}
w(LostPacket)	Probability of losing a packet for DoS level $i = 1, \ldots, 4$	0.001, 0.1, 0.15, 0.25
w(TxDelay)	Rate of transition of a packet for DoS level $i = 1, \ldots, 4$	$2 \cdot 10^{-i+1}$
β	Probability of DoS severity level transition (at each reconfiguration)	0.9

(modeling the packet delay depending on the progress of the DoS attack) for levels 1–4 are shown in Table 2 (the rate of a transition is the inverse of its mean delay).

In all experiments, the choice of these values assures that the DoS initial severity is the parameter with more impact on the measure of interest (i.e. the set of LCSs on which the reconfiguration function $RS_2()$ is computed). Obviously these values can be updated easily on the SWN model, because their update does not involve any change in the net structure.

EI-II interaction. As explained in Section 6, the presence of a DoS attack may alter the set of LCSs on which the reconfiguration function $RS_2()$ is computed, since due to the presence of a DoS a reconfiguration command may not reach one or more LCSs. We shall consider three cases of interaction:

Fixed Severity (FS) i. at each time t that an $RS_2()$ reconfiguration is computed the number of unreachable LCSs is drawn from the distribution of the number of unreachable substations at time t, assuming the SWN started at time 0 with a DoS severity s.

Probabilistically Increasing Severity (PIS). at each call of $RS_2()$ the severity level used in the SWN model can be either the same as in the previous call (with probability β) or it is increased by one (with probability $1 - \beta$).

Time Dependent Severity (TDS). in this case the SWN model is started at time 0 with a given severity level (the default is 1), and when at time t an $RS_2()$ function is applied the distribution at time t from the SWN model is used. As explained in Section 6 this requires a discretization of time in steps, in order to compute with the SWN a finite number of distributions (Note that this setting requires the use of a tool that allows us to acquire the reached simulated time, a feature that is possible within the SAN simulator facility of Möbius).

7.4. Analysis of the results

In this section we discuss the results of the analysis performed. To improve readability, only a subset of the power lines will be shown in the figures, selected among those that, according to the experiments, have a significant impact on the model behavior.

Fig. 5 shows the results of a first set of experiments, aimed at studying how different DoS situations impact on the unsupplied load. This experiment compares the behavior of the system for different choices of the failed line (x-axis), upon 6 different II behaviors, from the two extreme cases of no DoS with all LCS reachable (LCSR) and very severe DoS with all LCS unreachable (LCSU), through four cases of Fixed Severities (FS). Fig. 5 plots the percentage of undelivered load for time t equal to two days (UD for $t = 2d$), for the different failed power lines, identified by pairs $\langle n, n' \rangle$ of connected nodes. For each line, the 6 different II behaviors are plotted, left to right, following the top to bottom order of the legends.

Note that the impact of the DoS on the undelivered power strongly depends upon the failed line (the EI component), and ranges from a few percent to 20% depending on the severity of the DoS attack (the II component). When evaluating the reported measure it is important to remember that the results cover a fixed period of 48 h (2d) while the *average* DoS duration and the time to repair is 24 h (1d).

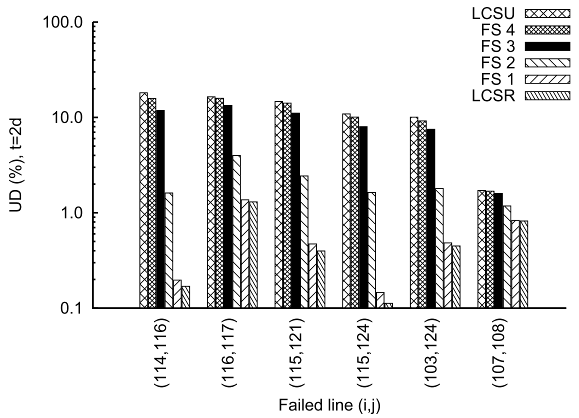

Fig. 5 – *UD* for different failed power lines, with fixed severity of DoS.

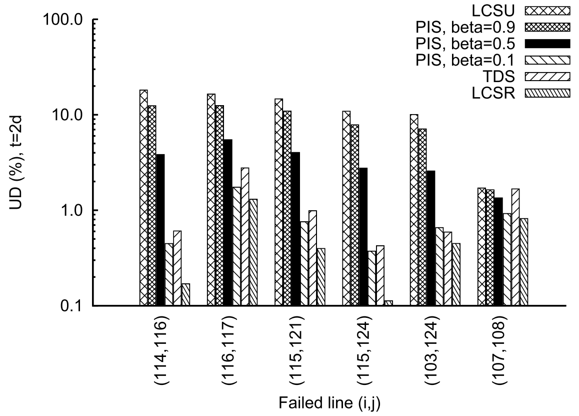

Fig. 6 – *UD* for different failed power lines, probabilistically increasing the DoS severity.

Fig. 6 reports UD when $t = 2d$ for the same failed power lines as in the previous figure, but now the DoS behaviors considered are the Time Dependent Severity (TDS) and what we have called the Probabilistically Increasing Severity case (PIS), where at each call of $RS_2()$ the DoS is assumed to have a severity increased by 1 with a probability β of 0.1, 0.5, 0.9, and the same severity as in the previous call with the complementary probability. Clearly, the greater the probability, the faster more and more LCS are considered unreachable. As before the two extreme cases (all reachable/all unreachable) have also been added for sake of reference. These cases have obviously the same values for both figures.

The two graphs of Figs. 5 and 6 consider the total load loss, thus providing a "grid's owner satisfaction" measure. The graph of Fig. 7 reports instead a "user satisfaction" viewpoint, since the load loss is computed for each load, which is an indicator of how the supplied service meets the customer demand during a single power line failure. The graph reports the percentage of power demand that is not met UD_i in a period of 2 days, considering the failure of the same 6 different power lines as for the previous graphs. Observe that

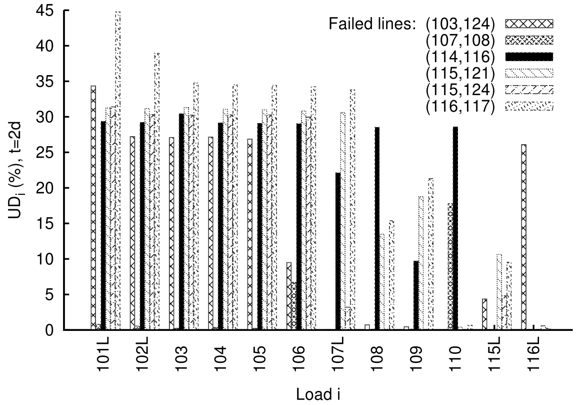

Fig. 7 – UD_i varying the failed power line, assuming that DoS severity increases very quickly ($\beta = 0.9$).

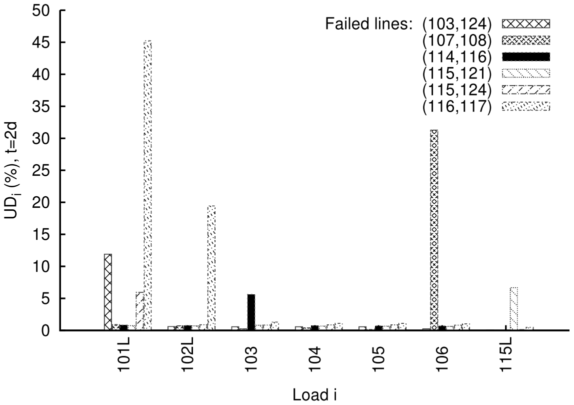

Fig. 9 – UD_i varying the failed power line, assuming that DoS is of type TDS.

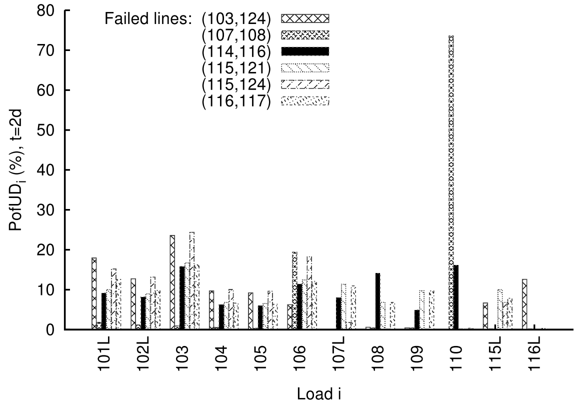

Fig. 8 – $PofUD_i$ varying the failed power line, assuming that DoS severity increases very quickly ($\beta = 0.9$).

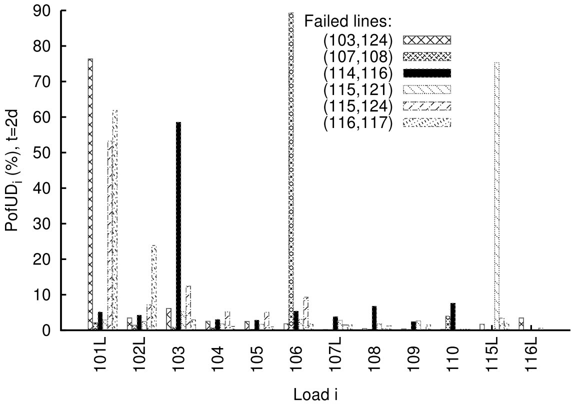

Fig. 10 – $PofUD_i$ varying the failed power line, assuming that DoS is of type TDS.

loads are affected quite differently, depending on the EI failed line, and that the worst case is about 50% of lost load for load 101*L*, when line (116,117) fails, which is quite a bad performance considering that the graph is over a period twice as long as the mean time to repair of the first failed power line. The graph in Fig. 7 assumes that the DoS is of type "PIS" with probability $\beta = 0.9$.

Since not all loads contribute in the same way to the total load of the system, we have investigated how each line contributes to the total undelivered load. Fig. 8 reports $PofUD_i$, the percentage of power demand that is not met for each load *i* with respect to total undelivered load. The setting is the same as for Fig. 7. Due to its definition, the sum over all loads of the bars of a given failed line sum up to 1. Again, there is a high variability: observe the load 110 in Fig. 8 and in Fig. 7. Upon failure of line (114,116), represented by the black bar, Fig. 7 reports that this failure provokes almost 30% shedding of load 110, and that a failure in line (114,116) is the worst failure for load 110. On the other side, when taking into account the contribution that load 110 gives to the entire load, it is clear from the graph in Fig. 8 that the most severe case is a failure in line (107,108). In fact, when such a failure occurs, due to the topology of the grid and related electric parameters, the contribution of load 110 to the total undelivered load amounts to almost 80%, while the contribution from the other loads is very low.

Figs. 9 and 10 report the same indices and the same setting of Figs. 7 and 8, but now the DoS behavior considered is what we have called the Time Dependent Severity (TDS). Note that a significant difference can be observed with respect to Figs. 7 and 8, since the highest percentage of lost load is now due to load 106, for a failure of line (107,108).

Figs. 11 and 12 take instead a different viewpoint, concentrating on a single load. Fig. 11 observes the percentage of undelivered load for a single load (load 101*L* in the figure) showing its variation as a function of the failed line and of the DoS behavior model, considering again the two extreme cases of all LCS reachable (LCSR case) and unreachable (LCSU), four values for fixed severity (1–4), the three cases of probabilistically increasing severity and the case of time dependent increasing severity.

Fig. 12 plots the contribution of load 101*L* to the total power loss ($PofUD_{101L}$) for the various DoS behaviors considered in the interactions. Again the high variability support the conjecture that a detailed modeling of the EI and II interaction is needed to have realistic results.

The last two figures provide another "system operator satisfaction" viewpoint, as it looks into the number of unsatisfied users, where each load is considered a single user

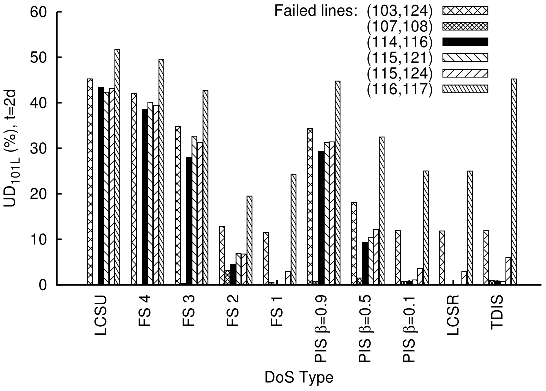

Fig. 11 – UD_{101L} as a function of the DoS behavior for different failed power lines.

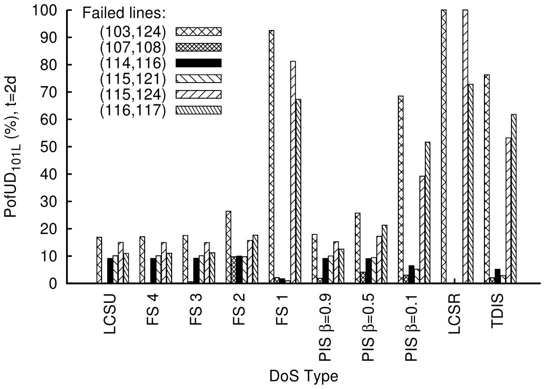

Fig. 12 – $PofUD_{101L}$ as a function of the DoS behavior for different failed power lines.

and a user is tagged as unsatisfied if the percentage of its own unsatisfied demand is above k% of its total request during the observed period (again from 0 to 2d). They do not plot the total number of users, but the percentage of unsatisfied users (loads) over the total number of users (loads), the *nlUDgtK* defined before (see Table 1).

In Fig. 13, it can be observed that, in the case of the failed line (103,124), about 80% of the users has experienced a reduction of supply with respect to its required load (case $k = 0$), and that about 10% has experienced a loss of more than 90% (case $k = 90$). This is the worst case for users unsatisfied to lose any percentage of requested demand. The failure with less impact on the percentage of unsatisfied users is that of line (107,108), which leads to more than 30% of the users with some unsatisfied demand, but only a few percentage (less than 5%) with a loss greater than 10.

Fig. 14 concentrates instead on a single failed line. Fig. 14 plots the percentage of unsatisfied users *nlUDgtK* for four different values of k, comparing the effect of the different DoS evolution types, upon failure of line (103,124). From the plot it is evident that a very high number of users is affected by the failure (from a minimum of 75% to a maximum of 95%) depending on how many LCS are reachable, and that depending of the type of DoS this loss can be limited or rather severe (compare the two extremes LCSU and LCSR for the case of at least 50% or 90% of users affected).

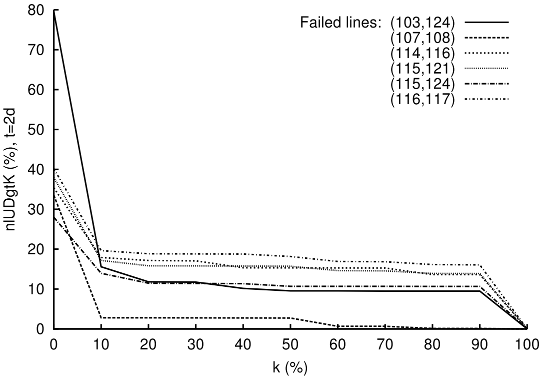

Fig. 13 – *nlUDgtK*, the percentage of loads whose unsatisfied demand is greater than k%, varying the failed power line and increasing the DoS severity very quickly (PIS, $\beta = 0.9$).

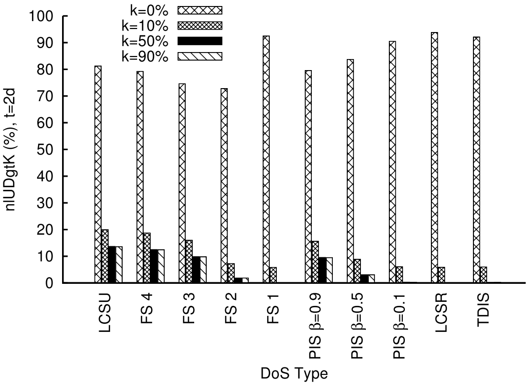

Fig. 14 – *nlUDgtK* as a function of the DoS behavior for different values of k and power line (103,124).

In summary, the plots show that, for the IEEE test grid, the effects on the users (loads) of a power failure can differ significantly depending on the starting severity of the DoS and on the speed at which the DoS propagates increasing its severity. A model taking into account only the electrical aspects will therefore fail to provide the system operator with an adequate picture of the impact of power failures.

8. Conclusions and future work

In this paper we have shown two different approaches to the modeling and quantification of the interplay between EI and II failures in a EPS. The two models have been instantiated on a specific scenario of cyberattack to the EPS: a DoS attack during a control teleoperation in which DSO and TSO cooperate in a load shedding activity.

Each approach focuses on a specific aspect and in this paper we have investigated how they can be synergistically integrated. The interaction is based on a computation, on the SWN model, of a set of distributions that are then used by the SAN model to characterize the DoS attack impact. We performed a large set of evaluations of the EPS behavior, that have addressed the quantification of the impact of different DoS attacks on indicators representative of the satisfaction of both users and system operators, e.g. the percentage of mean power demand that is not met in the interval $[0, t]$. Specifically, five different DoS attacks are analyzed, in conjunction with the failure of power lines of the "IEEE One Area RTS-96" test grid. The performed variety of analysis showed that the effects on the user satisfaction of a power line failure can differ significantly depending on the starting severity of the DoS and on the speed at which its severity increases. The results, although limited to the specific scenario and settings considered, point out the usefulness of such a study in understanding the dynamics of the involved failure phenomena, useful to take appropriate countermeasures to limit their effects on the user satisfaction.

In the presented work the SAN and SWN models have been kept separate. An alternative approach could be to extend the SAN model to embed into the SAN itself a submodel equivalent, or similar, to the SWN one. We see some drawback in this alternative: the simulation time will increase and the efficient SWN specific solution methods [5] could not be applied. Moreover, a modular approach should make it easier to experiment with different types of attacks, as far as they result in lost or delayed communications.

A positive side-effect of having precisely defined the interaction schema between the two models has been to point out the significant parameters of DoS attack state affecting the EI reconfiguration process after a failure.

Directions for future work include extensions of the integrated SWN-SAN analysis to consider other critical EPS scenarios where cyber attacks are involved in more sophisticated failures of the electric infrastructures, such as simultaneous failure of more power lines.

A further interesting research direction is represented by the integration of the results from cyber attack experiments, such as those presented in [37], to refine and validate the Petri net modeling the attack process and evaluate its impact.

REFERENCES

[1] CRUTIAL, European Project CRUTIAL — critical utility infrastructural resilience (contract n. 027513), http://crutial.rse-web.it.

[2] J.-C. Laprie, K. Kanoun, M. Kaâniche, Modeling interdependencies between the electricity and information infrastructures, in: SAFECOMP-2007, in: LNCS, vol. 4680, Springer Verlag, 2007, pp. 54–67.

[3] S. Donatelli, Dependent automata for the modelling of dependencies, in: Proc. of 3rd Int. Workshop on Critical Information Infrastructures Security, CRITIS 08, in: LNCS, vol. 5508, Springer Verlag, 2008, pp. 311–318.

[4] S. Baarir, M. Beccuti, D. Cerotti, M.D. Pierro, S. Donatelli, G. Franceschinis, The GreatSPN tool: recent enhancements, ACM Performance Evaluation Review 36 (4) (2009) 4–9. Spec. Issue on Tools for Perf. Eval..

[5] G. Chiola, C. Dutheillet, G. Franceschinis, S. Haddad, Stochastic well-formed coloured nets for symmetric modelling applications, IEEE Transactions on Computers 42 (11) (1993) 1343–1360.

[6] M. Beccuti, G. Franceschinis, M. Kaâniche, K. Kanoun, Multi-level dependability modeling of interdependencies between the electricity and information infrastructures, in: 3rd International Workshop on Critical Information Infrastructures Security, 2008.

[7] D. Daly, D.D. Deavours, J.M. Doyle, P.G. Webster, W.H. Sanders, 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, in: LNCS, vol. 1786, Springer Verlag, 2000, pp. 332–336.

[8] W.H. Sanders, J.F. Meyer, Stochastic activity networks: formal definitions and concepts, in: Lectures on Formal Methods and Performance Analysis, in: LNCS, vol. 2090, Springer Verlag, 2001, pp. 315–343.

[9] S. Chiaradonna, P. Lollini, F. Di Giandomenico, On a modeling framework for the analysis of interdependencies in electric power systems, in: IEEE/IFIP 37th Int. Conference on Dependable Systems and Networks, DSN 2007, Edinburgh, UK, 2007, pp. 185–195.

[10] M. Kaâniche, et al. The CRUTIAL modeling framework. Workpackage 2 Deliverable D16, CRUTIAL consortium, 2009.

[11] M. Beccuti, G. Franceschinis, S. Donatelli, S. Chiaradonna, F. Di Giandomenico, P. Lollini, G. Dondossola, F. Garrone, Quantification of dependencies in electrical and information infrastructures: the CRUTIAL approach, in: 4th International Conference on Critical Infrastructures, CRIS 2009, IEEE Computer Society Press, Linkoping, Sweden, 2009.

[12] S. Chiaradonna, F. Di Giandomenico, P. Lollini, Evaluation of critical infrastructures: challenges and viable approaches, in: Architecting Dependable Systems V, in: LNCS, vol. 5135, Springer Verlag, 2008, pp. 52–77.

[13] T.G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, John Wiley & Sons Inc., New Jersey, 2006.

[14] IRRIIS, European Project IRRIIS — integrated risk reduction of information-based infrastructure systems, http://www.irriis.org/.

[15] A. Nieuwenhuijs, E. Luiijf, M. Klaver, Modeling dependencies in critical infrastructures, in: M. Papa, S. Shenoi (Eds.), in: IFIP International Federation for Information Processing, vol. 290, Springer, Boston, 2009, pp. 205–213.

[16] R. Bloomfield, L. Buzna, P. Popov, K. Salako, D. Wright, 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, in: LNCS, vol. 6027, Springer, Berlin, Heidelberg, 2010, pp. 201–212.

[17] G. D'Agostino, R. Cannata, V. Rosato, On modelling of interdependent network infrastructures by extended Leontief models, in: E. Rome, R. Bloomfield (Eds.), 4th International Workshop on Critical Information Infrastructures Security, CRITIS 2009, in: LNCS, vol. 6027, Springer, Berlin, Heidelberg, 2010, pp. 1–13.

[18] E. Luiijf, A. Nieuwenhuijs, M. Klaver, M. Van Eeten, E. Cruz, Empirical findings on critical infrastructure dependencies in Europe, in: R. Setola, S. Geretshuber (Eds.), 3rd International Workshop on Critical Information Infrastructures Security, CRITIS 2008, in: LNCS, vol. 5508, Springer, Berlin, Heidelberg, 2009, pp. 302–310.

[19] R. Klein, 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, in: LNCS, vol. 5508, Springer, Berlin, Heidelberg, 2009, pp. 131–143.

[20] J. Chen, J.S. Thorp, I. Dobson, Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model, Electrical Power and Energy Systems 27 (4) (2005) 318–326.

[21] M. Anghel, K.A. Werley, A.E. Motter, Stochastic model for power grid dynamics, in: 40th Hawaii Int. Conference on System Sciences (CD-ROM), IEEE, Waikoloa, Big Island, Hawaii, 2007, pp. 113–122.

[22] S. Delamare, A.A. Diallo, C. Chaudet, High-level modelling of critical infrastructures' interdependencies, International Journal of Critical Infrastructures 5 (1/2) (2009) 100–119.

[23] B. Robert, R. De Calan, L. Morabito, Modelling interdependencies among critical infrastructures, International Journal of Critical Infrastructures 4 (4) (2008) 392–408.

[24] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S.D. Porcellinis, R. Setola, Modelling interdependent infrastructures using interacting dynamical models, International Journal of Critical Infrastructures 4 (1/2) (2008) 63–79.

[25] E. Casalicchio, E. Galli, S. Tucci, Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures, in: 11th IEEE International Symposium on Distributed Simulation and Real-Time Applications, 2007, pp. 182–189.

[26] W.H. Sanders, Progress towards a resilient power grid infrastructure, in: IEEE Power & Energy Society General Meeting, PES GM, Minneapolis, Minnesota, 2010.

[27] E. Bompard, R. Napoli, F. Xue, Analysis of structural vulnerabilities in power transmission grids, International Journal of Critical Infrastructure Protection 2 (1–2) (2009) 5–12.

[28] C.-W. Ten, C.-C. Liu, G. Manimaran, Vulnerability assessment of cybersecurity for SCADA systems, IEEE Transactions on Power Systems 23 (4) (2008) 1836–1846.

[29] R. Setola, How to measure the degree of interdependencies among critical infrastructures, International Journal of System f System Engineering (IJSSE) 2 (1) (2010) 38–59.

[30] S. Ruzzante, E. Castorini, E. Marchei, V. Fioriti, A metric for measuring the strength of inter-dependencies, in: E. Schoitsch (Ed.), SAFECOMP 2010, in: LNCS, vol. 6351, Springer, Berlin, Heidelberg, 2010, pp. 291–302.

[31] E. Casalicchio, E. Galli, Metrics for quantifying interdependencies, in: M. Papa, S. Shenoi (Eds.), in: IFIP International Federation for Information Processing, vol. 290, Springer, Boston, 2009, pp. 215–227.

[32] G. Dondossola, et al. ICT resilience of power control systems: experimental results from the CRUTIAL testbeds, in: 39th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 09, 2009, pp. 554–559.

[33] S. Chiaradonna, F. Di Giandomenico, P. Lollini, Definition, implementation and application of a model-based framework for the analysis of interdependencies in electric power systems, International Journal of Critical Infrastructure Protection (ijcip) 4 (1) (2011) 24–40.

[34] F. Romani, S. Chiaradonna, F. Di Giandomenico, L. Simoncini, 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, HASE'07, 2007, pp. 305–312.

[35] J.F. Meyer, Performability: a retrospective and some pointers to the future, Performance Evaluation 4 (3–4) (1992) 139–156.

[36] IEEE RTS task force of the APM subcommittee, the IEEE reliability test system — 1996, IEEE Transactions on Power Systems 14 (3) (1999) 1010–1020.

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