Multi-level dependability modeling of interdependencies between the Electricity and Information Infrastructures

M. Beccuti[1], G. Franceschinis[1], M. Kaâniche[2], and K. Kanoun[2]

[1] Dip. di Informatica, Univ. del Piemonte Orientale, 15100 Alessandria, Italy
{beccuti, giuliana}@mfn.unipmn.it
[2] LAAS-CNRS, Univ. de Toulouse, F-31077 Toulouse, France
{mohamed.kaaniche, karama.kanoun}@laas.fr

Abstract. The interdependencies between infrastructures may be the cause of serious problems in mission/safety critical systems. In the CRUTIAL[3] project the interdependencies between the electricity infrastructure (EI) and the information infrastructure (II) responsible for its control, maintenance and management have been thoroughly studied; moreover countermeasures to substantially reduce the risk to interrupt the service have been developed in the project. The possible interdependencies have been investigated by means of model at different abstraction levels. In this paper, we present high level models describing the various interdependencies between the EI and the II infrastructures, then we illustrate on a simple scenario how these models can be detailed to allow the evaluation of some measures of dependability.

1 Introduction

There is a wide consensus that developing modeling frameworks for understanding interdependencies among critical infrastructures and analyzing their impact is a necessary step for building interconnected infrastructures on which a justified level of confidence can be placed with respect to their robustness to potential vulnerabilities and disruptions. Modeling can provide useful insights into how component failures might propagate and lead to cascading, or escalating failures in interdependent infrastructures, and assess the impact of these failures on the service delivered to the users. In the context of CRUTIAL, we focus on two interdependent infrastructures: the electric power infrastructure (EI) and the information infrastructure (II) supporting management, business, control and maintenance functionality.

As discussed in [3], there has been extensive work on the modeling of individual infrastructures and various methods and tools have been developed to predict the consequences of potential disruptions within an individual infrastructure. However, the modeling and evaluation of interdependent infrastructures is

[3] CRUTIAL (Critical Utility Infrastructure resilience), FP6 European Project (http://crutial.cesiricerca.it)

still at an exploratory stage. The modeling activities carried out in CRUTIAL aim at contributing to fill this gap taking into account in particular: a) the three types of failures that are characteristic of interdependent infrastructures [6] (cascading[4], escalating[5], and common-cause failures), b) various classes of faults that can occur, including accidental as well as malicious threats, c) the temporal and structural characteristics of the power and information infrastructures investigated. A major challenge lies in the complexity of the modeled infrastructures in terms of largeness, multiplicity of interactions and types of interdependencies involved. To address this problem, a number of abstractions and appropriate approaches for composition of models are necessary. In CRUTIAL, the interdependencies have been analyzed at different levels: from a very abstract view expressing the essence of the typical phenomena due to the presence of interdependencies, to an intermediate detail level representing in a rather abstract way the structure of the system (in some scenarios of interest), to a quite detailed level where the system components and their interactions are modeled in a fairly realistic way and simulation is used to derive interesting reliability measures. In this paper a two-level modeling approach is proposed and illustrated through a simple scenario inspired by the CRUTIAL project. This is part of a multi-level and multi-formalism approach to the qualitative and quantitative study of the interdependencies between the EI and the II controlling and managing it.

In Section 2, the highest abstraction level is considered, showing the sequences of (abstract) events leading to typical interdependency phenomena such as cascading and escalation. In Section 3, a (simple) scenario is used to illustrate a more refined, second level representation, from which quantitative information can be provided to enable performance/reliability analysis. We will show how the higher level models can be composed with the more refined one and used to highlight possible instantiations of the abstract interdependencies phenomena. Section 4 concludes the paper.

2 High-level abstract models of interdependencies

This section summarizes the high-level abstract models presented in [5]. We model the EI and II behavior globally, taking into account the impact of failures in the infrastructures, and their effects on both infrastructures, without taking into account explicitly their underlying implementation structure. For sake of clarity, events and states of the II are prefixed by **i-** while those of the EI are prefixed by **e-**. We first address accidental failures in II, then malicious attacks.

[4] Cascading failures occur when a failure in one infrastructure causes the failure of one or more component(s) in a second infrastructure

[5] Escalating failures occur when an existing failure in one infrastructure exacerbates an independent failure in another infrastructure, increasing its severity or the time for recovery and restoration from this failure

2.1 Accidental failure model

The model, given in Fig. 1, is based on assumptions related to the behavior of the infrastructures as resulting from their failures and mutual interdependencies. These assumptions are summarized, before commenting the model.

Impact of i-failures. Accidental i-failures, affecting the II can be either masked (unsignaled) i-failures, leading to latent errors, or signaled. Latent errors can be either passive (i.e., without any action on the EI, but keeping the operators uninformed of possible disruptions occurring in the EI) or active (provoking undue configuration changes in the EI). After signaled i-failures, the II is in a partial i-outage state. Latent errors can accumulate. Signaled i-failures may take place when the II is in latent error states. When the II is in a partial i-outage state, i-restoration is necessary to bring it back to an i-working state. We assume that an i-failure puts some constraints on the EI (i.e., cascading failure), leading to a weakened EI (e.g., with a lower performance, unduly isolations, or unnecessary off-line trips of production plants or of transmission lines). From an e-weakened state after a signaled i-failure, an e-configuration restoration leads EI back into a working state, because no e-failures occurred in the EI. Accumulation of untimely configuration changes, may lead to e-lost state (i.e., a blackout state), from which an e-restoration is required to bring back the EI into an e-working state. The above events and the resulting states are recapitulated in Table 1.

Impact of e-failures. We consider that the occurrence of e-failures leads the EI to be in a partial e-outage state, unless propagation within the infrastructure leads to losing its control (e.g., a blackout of the power grid) because of an i-failure (this latter case corresponds to escalating events). Also e-failures may lead the II to an i-weakened state in which parts of the II can no longer implement their functions, although they are not failed, due to constraints originating from the failure of the EI. The above events and the states are recapitulated in Table 2.

2.2 Malicious attacks model

Attacks fall into two classes: deceptive attacks provoking unperceived malfunctions, thus similar to the latent errors previously considered, and perceptible attacks creating detected damages. Deceptive attacks can be passive (i.e., without any direct action of the II on the EI) or active, provoking configuration changes in the EI, by the II.

Fig. 2 gives the state machine model of the infrastructures. Due to the very nature of attacks, a distinction has to be performed for both infrastructures between their real status and their apparent status. For the EI, the apparent status is as reported by the II. Models of Figs. 1 and 2 are very similar: they differ by the semantics of the states and of the inter-state transitions.

In state 2, the effects of the passive deceptive attack are: i) the II looks like working while it is in a partial i-outage state due to the attack, ii) it does not perform any action on the EI, but informs wrongly the operator that the

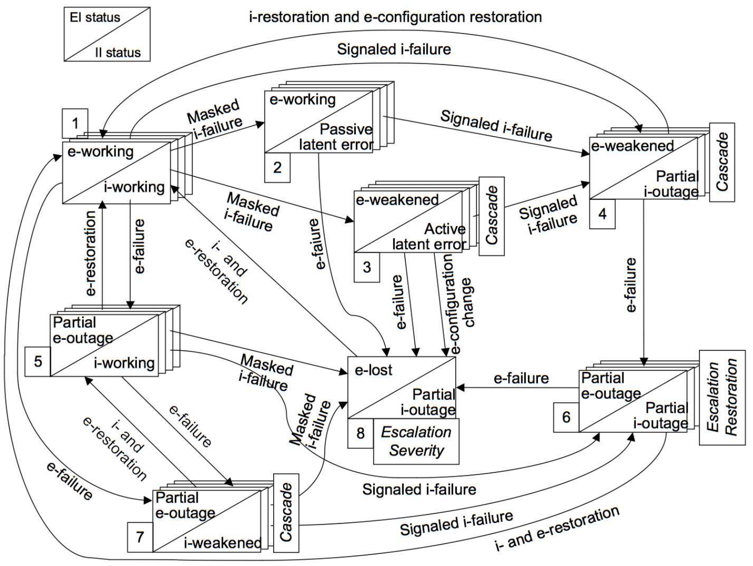

Fig. 1. Model of the two infrastructures when considering accidental failures.

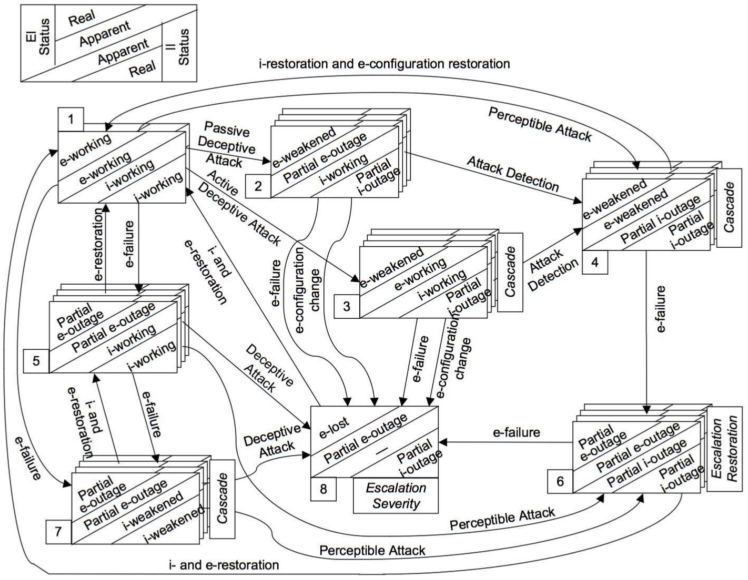

Fig. 2. Model of the two infrastructures when considering malicious attacks.

Events	
Signaled i-failure	Detected i-failure.
Masked i-failure	Undetected i-failure.
i-restoration	Action for bringing back the II in its normal functioning after i-failure(s).
States	
i-working	The II ensures normal control of the EI.
Passive latent error	Parts of the II have an i-failure, which prevents monitoring of the EI: e-failures may remain unnoticed.
Active latent error	Parts of the II have an i-failure, that may lead to unnecessary, and unnoticed configuration changes.
Partial i-outage	Parts of the II have knowingly an i-failure. Partial i-outage is assumed: the variety of functions and of the components of the infrastructure, and its essential character of large network make unlikely total outage.
i-weakened	Parts of the II can no longer implement their functions, although they do not have an i-failure, due to constraints originating from e-failures (e.g., shortage of electricity supply of unprotected parts).

Table 1. States and events of the information infrastructure (II).

Events	
e-failure	Malfunctioning of elements of the power grid: production plants, transformers, transmission lines, breakers, etc.
e-restoration	Actions for bringing back the EI in its normal functioning after e-failure(s) occurred. Typically, e-restoration is a sequence of configuration change(s), repair(s), configuration restoration(s).
e-configuration change	Change of configuration of the power grid that are not immediate consequences of e-failures, e.g., off-line trips of production plants or of transmission lines.
e-configuration restoration	Act of bringing back the EI in its initial configuration, when configuration changes have taken place.
States	
e-working	Electricity production, transmission and distribution are ensured in normal conditions.
Partial e-outage	Due to e-failure(s), electricity production, transmission and distribution are no longer ensured in normal conditions, they are however somehow ensured, in degraded conditions.
e-lost	Propagation of e-failures within the EI led to losing its control, i.e., a blackout occurred.
e-weakened	Electricity production, transmission and distribution are no longer ensured in normal conditions, due to i-failure(s) of the II that constrain the functioning of the EI, although no e-failure occurred in the latter. The capability of the EI is degraded: lower performance, configuration changes, possible manual control, etc.

Table 2. States and events of the electricity infrastructure (EI).

EI is in partial e-outage, and as consequence iii) the operator performs some configuration changes in the EI leading it to an e-weakened state. Accumulation of configuration changes by the operator may lead the EI into e-lost state.

In state 3, the effects of the active deceptive attack are: i) the II looks like working while it is in a partial i-outage state due to the attack, ii)it performs some configuration changes in the EI leading it to an e-weakened state without informing the operator, for whom the EI appears as if it were working. Accumulation of configuration changes by the II may lead the EI into a e-lost state. The difference between states 2 and 3 is that in state 2 the operator has made some actions on the EI, while in state 3 the operator is not aware of the actions performed by the II on the EI.

After detection of the attack, the apparent states of the infrastructures become identical to the real ones (state 4), in which i-restoration and e-configuration restoration are necessary to bring back the infrastructures to their working states. States 5, 6 and 7 are very similar respectively to states 5, 6 and 7 of Fig. 1, except that in state 6 the II is in a partial i-outage state following a perceptible attack in Fig. 2 and following a signaled i-failure in Fig. 1. State 8 corresponds to e-lost state but the operator is not aware, he has been informed wrongly by the partial i-outage of II that it is in a partial e-outage state.

2.3 Global conceptual model

The global abstract model, taking into account both accidental failures and malicious attacks, results from the superposition of the two models. In [4], a unified model is presented. In this paper we have presented the separate models for sake of simplicity. Our aim is to illustrate how to join the abstract modeling level to detailed models allowing dependability quantification.

3 Detailed models of scenarios

The high level abstract models show typical failure scenarios and the combined states of the infrastructures as resulting from their interdependencies. The evaluation of quantitative dependability measures based on these models requires the specification of the probability distributions associated with the transitions of the abstract models. As these transitions result from the occurrence of several elementary events affecting the components of the infrastructures, the development of more detailed models highlighting these events and taking into account the internal behavior of the infrastructures should help to identify representative probability distributions. States in Fig. 1 and 2 are in reality macro states gathering a set of elementary states of the infrastructures in which the service delivered is equivalent. Let us for example consider the transition from state 1 to state 4 in Fig. 1. This transition takes place only when the accumulation of elementary events result in a significant degradation of the service delivered by EI, leading it to an “e-weakened state”.

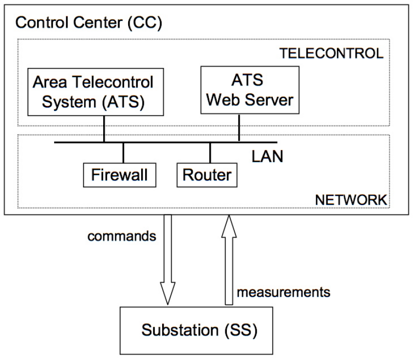

Fig. 3. Architecture of the EI and II considered for the example

Quantification of dependability measures requires to model the underlying systems behavior. A measure of dependability could be for example the distribution of the time to reach state 4 from state 1, either directly or through states 2 and 3, i.e., the distribution of the time to a signaled failure (Fig. 1), or the distribution of the time to a perceptible attack (Fig. 2).

In this section, we show a simple example of a detailed model allowing the evaluation of this distribution. We will describe the underlying system and its associated models and show the relationship between the detailed and the high-level abstract model.

3.1 A more detailed model of a simple scenario

The system considered is described in [2] and it is illustrated in Fig. 3. It represents the teleoperation function performed between a Control Centre (CC) and a SubStation (SS), by means of a communication network. We suppose that the communication between the sites is performed in the following way: the CC sends requests to the SS to obtain the execution of a command by the SS (e.g., arming), or to retrieve data from the SS (signals, measures, etc.). The SS replies to the CC by acknowledging the command execution, or by sending the required data. Each communication needs a minimum level of available bandwidth to be completed. In this context we consider two types of i-failures, bringing the system from state 1 to state 4 of Figs 1 and 2 models, respectively.
1. A signaled i-failure of the CC that can occur in the two following cases: the TELECONTROL devices (ATS or ATS Web Server) are not available or the communication inside the CC is not available due to the failure of either Local Area Network (LAN, Firewall and Router).
2. A perceptible denial of service (DoS) attack to the communication network. Such attack consists of sending a high number of packets on the communication network, with the effect of reducing the available bandwidth and causing exces-

sive delay or loss of packets between CC and SS. A DoS attack may last for a random period of time, and it may be blocked by the success of a countermeasure (firewalling, traffic monitoring, etc.).

3.2 Description of the model

For modeling the above scenario we use a multi-formalism combining the Stochastic Well-formed Net (SWN) [1] and Fault Tree (FT) [7] formalisms. In particular, the multi-formalism model is composed by two submodels: an SWN model and an FT model. The first is an SWN model (Fig. 4), which represents the exchange of requests and replies between the CC and the SS by means of the communication network, and the possibility of the occurrence of a DoS attack on the same network. Instead the second one, a FT model (Fig. 5), represents the failure mode of the CC.

The SWN is an High Level Stochastic Petri Net formalism. Places (circles) containing tokens (which in HLPN can carry information) represent the state, while transitions (boxes) represent state changes whose preconditions and effects are represented by arcs. Transition firing times are random variables. The fact that tokens can carry information make the model parametric: e.g. each message can have a distinct identifier, moreover the model can be easily extended to represent several SS. Finally, SWN models can be studied through very efficient analysis techniques exploiting the presence of symmetries in the model.

SWN model description. The SWN model is shown in Fig. 4 where the dashed boxes represent the CC, the SS and the attacker respectively. The transition *CC_send* models the generation of a request to be sent to the SS, by putting a token inside the place *CC_buffer_out* and inside the place *Commands* describing the requests to be sent on the network, and the requests waiting for a reply, respectively. The bandwidth is modeled by a set of tokens inside the place *Bandwidth*; each time a request has to be sent (a token is present in *CC_buffer_out*), the marking of Bandwidth is reduced by one for modeling the reduction of bandwidth due to the transmission (transition *CC_transmit*).

When the transition *CC_transmit* fires, the token representing the request is moved from the place *CC_out* to the place *SS_buffer_in*, in order to model the receipt of the request by the SS. Moreover, the firing of *CC_transmit* determines the increase of the marking of the place Bandwidth, in order to model the fact that more bandwidth is now available.

The requests to be processed by the SS are represented by tokens inside the place *SS_buffer_in*. The processing is modeled by the transition *process*. The replies are represented by tokens put inside the place *SS_buffer_out*; their transmission is represented by the transition *SS_transmit*; as in the case of the requests, the transmission of replies determines a temporary decrease of the marking of the place *Bandwidth*. Once the reply is received by the CC (token inside the place *CC_buffer_in*), the corresponding pending request is removed from the place *Commands*.

The failure event of the CC is modeled by transition *CC_fail*: its firing time distribution is given by the FT. The firing of such transition leads to the marking

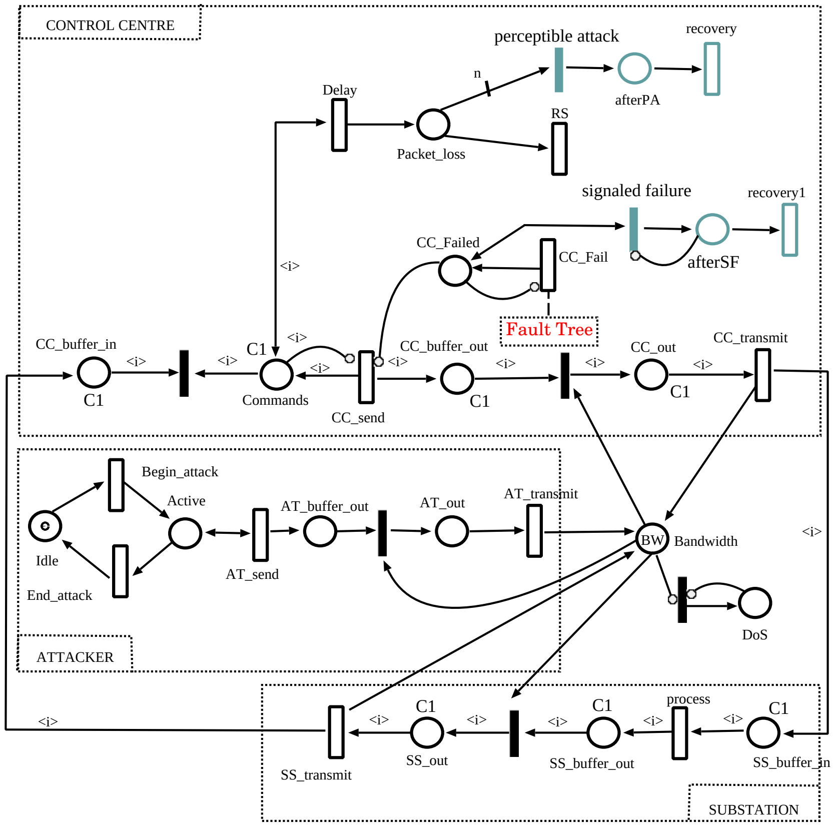

Fig. 4. SWN model representing the exchange of requests and replies between the CC and the SS by means of the communication network.

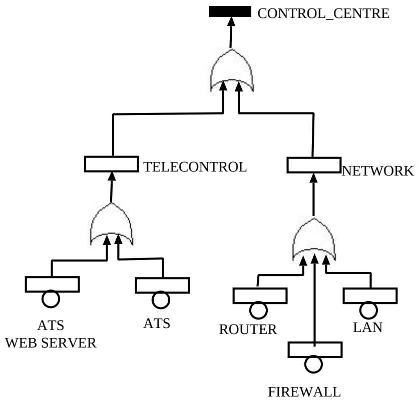

Fig. 5. FT model representing the failure mode of the CC.

of the place *CC_failed* modeling the state of failure. The marking of *CC_failed* causes the inhibition of the transition *CC_send*.

The attacker state is modeled by the places *Idle* and *Active*; the initial state is idle, but it can turn to active after the firing of the transition *Begin_attack*. In the active state, the attacker generates packets (transition *AT_send*) to be transmitted on the communication network (transition *AT_transmit*). As in the case of the transmission of requests and replies, the transmission of the attacker packets determines the reduction of the marking of the place *Bandwidth*. The complete unavailability of the bandwidth (the success of the DoS attack) is modeled by the place *DoS* becoming marked when no tokens are present in the place *Bandwidth*. The state of the attacker can turn back to idle if the transition *End_attack* fires representing the discovery of the attack by some countermeasure. The loss of replies is modeled by the timed transition *Delay*: if a token (pending request) stays inside the place *Commands* for a long time (the corresponding reply has not been received during that time), the transition *Delay* may fire leading to the marking of the place *Packet_loss* modeling the loss of a reply. Moreover, transition *RT* removes a token from the place *Packet_loss*.

Finally the transitions *perceptible attack*, *signaled failure*, *recovery* and *recovery1*, and the places *afterPA* and *afterSF* are used for mapping this model on the abstract model (Sect. 2), as we will describe in details in the next section.

FT model description. Fig. 5 shows the FT model representing the failure mode of the CC. Such failure is represented by the top event called *CONTROL_CENTRE*. Such event is the output of an OR gate whose inputs are the event *TELECONTROL* and *NETWORK*; therefore, the top event (the CC failure) occurs if the telecontrol function or CC network fails. The event *TELECONTROL* represents the failure of the telecontrol devices; such event is the output of an OR gate having *ATS* and *ATS_WEB_SERVER* as input events. Therefore the event *TELECONTROL* is caused by the failure of the *ATS* or by the failure of *ATS_WEB_SERVER*. Finally the *NETWORK* fails if the *ROUTER*, the *FIREWALL* or the *LAN* fails.

3.3 Interpretation of the model measures w.r.t. the abstract model

The abstract model introduced in Sect. 2 allows capturing at a high abstraction level the interesting interdependency phenomena. The example introduced in Sect. 3.2 can be mapped on the abstract model as follows:

1. The signaled i-failure in the CC is triggered by the firing of the transition *CC_failed* whose firing time is controlled by the FT model.

2.The perceptible attack corresponds to a loss of responsiveness due to a DoS attack and is modeled by a transition firing activated when n commands are lost in a short period. Observe that in the model command messages (and the corresponding acknowledgments) are never actually lost, however if the acknowledgment of a transmitted command arrives later than a specified maximum amount of time, this is interpreted as a command loss. This mechanism is implemented by introducing a *Delay* transition, activated when a command has been sent from the CC, and working as a timeout used to record an excessive delay of the command acknowledge. When *Delay* fires, another timeout starts to count, which is used to forget about command/acknowledge losses after a certain time since their occurrence. If the model manages to accumulate enough (n) command losses before they expire, this is interpreted as an indication that some misbehavior is happening which should be signaled.

The connection between the detailed and abstract models can be performed in different ways: the first option is to define a correspondence among states: so for example we could say that all states with at least one token in place $afterPA$ or in place $afterSF$ correspond to state 4 while all states where these two places are not marked correspond to state 1. So to compute the distribution of the time required to reach abstract state 4 from abstract state 1 can be performed on the detailed model by simply making the states with $m(afterPA)+m(afterSF) > 0$ as absorbing and computing on the model the distribution of the time to absorption. If we consider also the possibility of restoration (which for the moment is represented in the detailed model as two simple "reset" transitions, called *recovery* and *recovery*1, which bring the whole net back to the initial state), then we can also compute steady state behavior measures, e.g., the probability of being in state 1 or 4.

The alternative way to couple the two models is by making a correspondence between the transitions: in this example this is particularly simple because transitions "Signaled failure" and "Perceptible attack" (as well as “recovery” and“recovery1”) can be directly put in correspondence with the homonymous transitions in the abstract model: in this case the mapping among the states is indirect (but can be made explicit by adding some “implicit places” in the detailed model representing the abstract model states and connect them to the matching transitions).

Finally, in order to compute performance measures it is necessary to associate a firing delay probability distribution with every timed transition in the detailed model. These firing delay probability distributions can be deduced from experimental data obtained both by real system behavior observation and by testbed simulation. After that, if all these distributions can be expressed by negative exponential distributions then the system performance measures can be computed by numerical analysis, else by simulation.

4 Conclusion and perspective

This paper presented a dependability modeling approach that takes into account interdependencies related failures affecting electrical infrastructures and associated information infrastructures supporting e.g., management, control and monitoring activities. Two abstraction levels are considered. At the highest level, each infrastructure is modeled globally as a black box and the proposed models identify cascading and escalating related failure scenarios and corresponding service restoration actions resulting from accidental failures or malicious attacks. The failure scenarios highlighted at this abstraction level result from the occurrence and propagation of elementary events originating from the subsystems and components of the infrastructures.

The development of detailed models taking into account the structure and the internal behaviour of the infrastructures is useful to link the elementary failure events to the high level scenarios of cascading and escalating failures. Also, the detailed models can contribute to the definition of the probability distributions to be associated with the transitions in the high level abstract model to evaluate quantitative measures characterizing the impact of interdependencies with regards to the occurrence of blackouts. One of the critical issues that need to be addressed in this context is the mapping of the detailed models to the high-level abstract models. The example presented in this paper, inspired from a case study investigated in CRUTIAL, is aimed at illustrating how this mapping can be achieved and how the effects of accidental and malicious failures can be analyzed together.

So far we have considered simple scenarios. More complex detailed models are currently investigated, taking into account the main subsystems and components of both the electrical and the information infrastructures. Two other possible directions of future work are: (1) the compositional construction of the higher abstraction level models from submodels of the two infrastructures highlighting the cause-effect relations between events: this can be done either using automata or using Petri Nets (the latter choice would also ease the successive composition with lower level PN models), (2) adding a further level of detail (typically corresponding to accurate simulation models) from which the quantitative parameters of the intermediate level models can be deduced when direct measures from true systems are not available.

Acknowledgment. This work is partially funded by the European Commission through the CRUTIAL project. All our thanks to Jean Claude Laprie who developed the main concepts behind the abstract model of interdependencies used in this paper.

References

1. G. Chiola, C. Dutheillet, G. Franceschinis, and S. Haddad. Stochastic well-formed coloured nets for symmetric modelling applications. *IEEE Transactions on Computers*, 42(11):1343–1360, nov 1993.
2. F. Garonne et al. *Analysis of new control applications*, 2007. Crutial Deliverable D2, http://crutial.cesiricerca.it/Dissemination.
3. M. Kaâniche et al. *Methodologies Synthesis*, 2007. Crutial Deliverable D3, http://crutial.cesiricerca.it/Dissemination.
4. M. Kaâniche et al. *Preliminary modelling framework*, 2008. Crutial Deliverable D8, http://crutial.cesiricerca.it/Dissemination.
5. J-C Laprie, K. Kanoun, and M Kaaniche. Modelling interdependencies between the electricity and information infrastructures. In *6th Inter Conf. on SAFECOMP'2007*, pages 54–67, Nuremberg (Germany), September 2007. Springer, LNCS 4680-0054.
6. S.M Rinaldi, J.P. Peerenboom, and T.K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 42(11):11–25, December 2001.
7. W.G. Schneeweiss. *The Fault Tree Method*. LiLoLe Verlag, 1999.