Project no.:	**IST-FP6-STREP - 027513**
Project full title:	**Critical Utility InfrastructurAL Resilience**
Project Acronym:	**CRUTIAL**
Start date of the project:	**01/01/2006 Duration: 36 months**

Deliverable no.: D3

Title of the deliverable: Methodologies synthesis

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Contractual Date of Delivery to the CEC:	**31/12/2006**
Actual Date of Delivery to the CEC:	**17/01/2007**
Organisation name of lead contractor for this deliverable	**LAAS-CNRS**
Author(s): M. Kaâniche[4] (Editor), S. Bernardi[6], A. Bobbio[6], C. Brasca[1], S. Chiaradonna[3], D. Codetta Raiteri[6], F. Di Giandomenico[3], G. Dondossola[1], G. Franceschinis[6], F. Garrone[1], A. Horvath[6], K. Kanoun[4], J.C. Laprie[4], P. Lollini[3], J. Sproston[6]	
Participant(s): [4]LAAS-CNRS, [6]CNIT, [3]CNR-ISTI, [1]CESI	
Work package contributing to the deliverable:	**WP2**
Nature:	**R**
Dissemination level:	**PU**
Version:	**3.0**
Total number of pages:	**76**

Abstract:

This deliverable deals with the modelling and analysis of interdependencies between critical infrastructures, focussing attention on two interdependent infrastructures studied in the context of CRUTIAL: the electric power infrastructure and the information infrastructures supporting management, control and maintenance functionality. The main objectives are: 1) investigate the main challenges to be addressed for the analysis and modelling of interdependencies, 2) review the modelling methodologies and tools that can be used to address these challenges and support the evaluation of the impact of interdependencies on the dependability and resilience of the service delivered to the users, and 3) present the preliminary directions investigated so far by the CRUTIAL consortium for describing and modelling interdependencies.

Keyword list:. critical infrastructures, power systems, interdependencies modelling, dependability and security evaluation

DOCUMENT HISTORY

Date	Version	Status	Comments
15/09/2006		Draft	First version of Table of contents
17/10/2006		Draft	Table of contents agreed
15/11/2006		Draft	Partners contributions to the different sections
30/11/2006	V0	Draft	First integrated version, ready for internal review by involved partners
18/12/2006	V1	Draft	Second integrated version including comments received on first integrated version and additional improvements
24/12/2006	V2	Draft	Third integrated version including comments received on second integrated version and additional improvements, distributed to all project members for final review.
15/12/2006	V3	Final	Integration of final comments and production of final version delivered to EC.

Table of Contents

1 INTRODUCTION

In the past 40 years, the electric power grid in several countries all over the world experienced multiple cascading failures that affected the power supply to millions of customers. The most recent one occurred on November 4 this year in Western Europe when a shutdown of a high-voltage line in Germany resulted in massive power outages in France and Italy as well as in parts of Spain, Portugal, the Netherlands, Belgium and Austria, and even extended as far as Morocco. About 10 million customers in Europe were affected by this failure. Similar major blackouts with even more severe consequences have occurred in the summer 2003 in the United States, in Canada and in Italy [US-Canada 2004, Pourbeik *et al.* 2006]. These events highlight the vulnerability of the electric grid infrastructures and their interdependencies. The large geographic extension of power failures effects is related to the high interconnectivity of power grid transmission and distribution infrastructures and the multiple interdependencies existing between these infrastructures and the information infrastructures supporting the control, the monitoring, the maintenance and the exploitation of power supply systems. Clearly there is a need to analyze and model critical infrastructures in the presence of interdependencies in order: i) to understand how such interdependencies may contribute to the occurrence of large outages and blackouts and ii) to develop architectural solutions that are well suited to improve the dependability and resilience of power grid infrastructures.

The CRUTIAL project aims to address these objectives focussing attention on two interdependent infrastructures: the electric power infrastructure and the information infrastructures supporting management, control and maintenance functionality. Starting from the existing electric power infrastructure, the project aims to investigate new approaches that are well suited to cope with the recent market deregulation in the context of distributed and renewable energy resources, the dramatic increase of power demand, and the advent on new threats caused in particular by the increased openness of the information infrastructures and the multiplication of actors and stakeholders in the management and exploitation of the system [Amin 2005].

There is a consensus in the literature on critical infrastructures that interdependency analyses and models constitute a necessary step [Rinaldi *et al.* 2001]. The International CIIP Handbook 2004 [Wenger *et al.* 2004] is a comprehensive collection of information about the various initiatives undertaken by the different countries on the theme of Critical Information Infrastructure Protection (CIIP), mainly at governmental level. The CIIP Handbook underlines the need of developing methodologies for analyzing interdependencies and guiding the protection of critical information infrastructures.

This deliverable focuses on the modelling and analysis of interdependencies. The main objectives are: 1) investigate the main challenges to be addressed for the analysis and modelling of interdependencies, 2) review the modelling methodologies and tools that can be used to address these challenges and support the evaluation of the impact of interdependencies on the dependability and resilience of the service delivered by power system infrastructures, and 3) present the preliminary directions investigated so far by the CRUTIAL consortium for describing and modelling interdependencies.

The structure of the deliverable is as follows. Section 2 discusses the problems and challenges raised by interdependencies from the assessment and evaluation perspectives. Section 3 reviews existing model-based methodologies, techniques and tools that can be useful to address the challenges reported in Section 2, and summarizes related work and cooperative projects dealing with the modelling and evaluation of interdependent critical infrastructures in general, and power system infrastructures in particular. Preliminary directions about the approach followed in CRUTIAL for interdependencies modelling are discussed in Section 4. This section is organised into two subsections. The first subsection 4.1 presents qualitative models for describing the typical failures that are

characteristic of interdependent infrastructures, i.e., cascading, escalating and common-cause failures. The infrastructure interdependencies are modelled globally without explicitly describing their component behaviours. The detailed modelling of the infrastructures taking into account their internal structure is discussed in subsection 4.2 where a preliminary hierarchical modelling framework is presented based on the architectural descriptions and scenarios presented in [Brasca *et al.* 2006, CESI RICERCA 2006b, Leuven 2006]. Finally, Section 5 of this deliverable presents the main conclusions and indications for future work.

2 INTERDEPENDENCIES - BACKGROUND AND CHALLENGES

Interdependencies give rise to numerous challenges that need to be taken into account to build useful models that reflect the complex phenomena affecting the dependability and the resilience of the infrastructures under investigation. In this section, we review some of these challenges, starting with the definition of concepts and terminology related to interdependencies, based in particular on the seminal work presented in [Rinaldi *et al.* 2001]. For dependability concepts, the reader is referred to [Avizienis *et al.* 2004].

2.1 Interdependencies definitions and concepts

Critical infrastructures are complex collections of interacting systems and components communicating through multiple heterogeneous networks. The interactions between these components and systems need to be analyzed carefully to understand and characterize the interdependencies.

An *interdependency* is a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent if each is dependent on the other.

Infrastructure interdependencies can be categorized according to various dimensions in order to facilitate their identification, understanding and analysis. Six dimensions have been identified in [Rinaldi *et al.* 2001] (see Figure 1). They include the type of interdependencies (physical, cyber, geographic, and logical), the infrastructure environment (technical, business, political, Legal, etc.), c) the couplings among the infrastructures and their effects on their response behaviour (loose or tight, inflexible or adaptive), and d) the infrastructure characteristics (organisational, operational, temporal, spatial), the state of operation (normal, stressed, emergency, repair), the degree to which the infrastructures are coupled, the type of failure affecting the infrastructures (common-cause, cascading, escalating).

In the following, we briefly discuss the key factors covered by these different dimensions, focussing on the type of interdependencies, the infrastructures characteristics, the types of failures and threats, and finally the service modes and operation states.

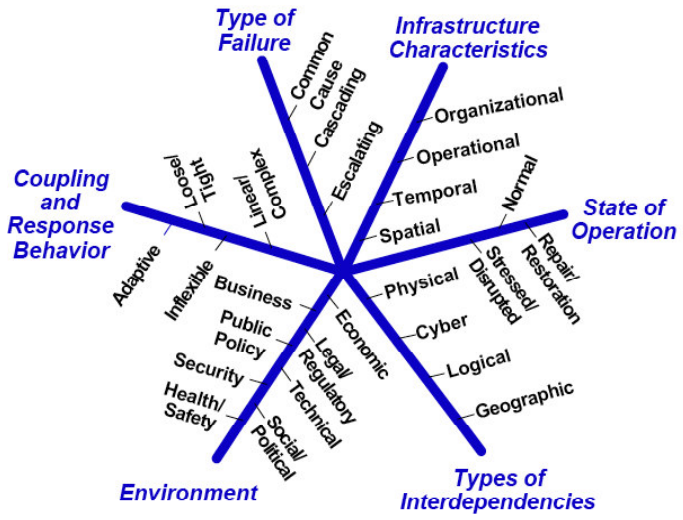


Figure 1: Interdependencies dimensions (source [Rinaldi 2004])

2.1.1 Types of interdependencies

Four classes of interdependencies have been distinguished in [Rinaldi *et al.* 2001]: Physical, cyber, geographic, and logical.

- *Physical interdependencies* arise from physical linkages or connections among elements of the infrastructures. In this context disruptions and perturbations in one infrastructure can propagate to other infrastructures.

- *Cyber interdependencies* occur when the state of an infrastructure depends on information transmitted through the information infrastructure. Such interdependencies result from the increased use of computer-based information systems such as SCADA systems, to support control, monitoring and management activities

- *Geographic interdependencies* exist between two infrastructures when a local environmental event can create state changes in both of them. This generally occurs when the elements of the infrastructures are in close spatial proximity.

- *Logical interdependencies* gather all interdependencies that are not physical, cyber or geographic, caused for example by regulatory, legal or policy constraints.

The four types of interdependencies are not mutually exclusive, although each of them has its own characteristics. Other classifications have also been proposed in the literature [Masera 2002, Lee *et al.* 2004, Pederson *et al.* 2006]. For example, the classification proposed in [Masera 2002] looks at both the involved systems and their potential interconnections that are characterized by two key factors:

- the character of the link that identifies which elements of the systems are affected: physical, logical, human/organizational;

- the layer of interaction: structural, functional, behavioural.

This classification has been used in the paper as a basis for discussing the problem of interdependencies among systems and their impact on dependability assessment, taking as an example the interconnections between power and communication infrastructures.

2.1.2 Infrastructure characteristics

In the analysis of interdependencies, several characteristics of the infrastructures under investigation need to be examined. These concern in particular the structural composition of the infrastructures and their temporal dynamics.

The infrastructures are generally composed of a large number of interconnected systems and components with multiple interactions between them. Clearly, it is not recommended to examine the infrastructures at a high level of detail due to the complexity of these infrastructures. It is necessary to find the right level of detail and abstraction at which the interdependencies should be examined. The right level can be determined by the types of behaviours one would like to look at, the quantitative measures to be evaluated, and the information available to characterize the relevant phenomena that have the most significant impact on the dependability of the interdependent infrastructures, in particular with respect to the occurrence of cascading, escalating or common cause failures.

The study of the temporal dynamics of the infrastructures might also be important for the analysis of interdependencies. Indeed, the activities supported by the infrastructures to accomplish the required services and to react to error conditions and failures can span a vast temporal range. Some phenomena may be pertinent to the analysis of interdependencies only if they occur and persist beyond a given period of time. For instance, some error propagation scenarios between infrastructures might occur only if the effects of some failures cannot be confined and recovered very quickly. Time scales have also implications on the modelling, especially when a large variation exists between the order of magnitudes of some parameters included in the models (see Section 2.2 for further discussion).

2.1.3 Types of failures and threats

Interdependencies increase the vulnerability of the corresponding infrastructures as they give rise to multiple error propagation channels from one infrastructure to another that make them more prone to exposure to accidental as well as to malicious threats. Consequently the impact of infrastructure components failures and their severity can be exacerbated and are generally much higher and more difficult to foresee, compared to failures confined to single infrastructures. As an example, most major power grid blackouts that have occurred in the past are initiated by a single event (or multiple related events such as an equipment failure of the power grid that is not properly handled by the SCADA system) that gradually leads to cascading outages and eventual collapse of the entire system [Pourbeik *et al.* 2006].

Three types of failures are of particular interest when analyzing interdependent infrastructures: 1) cascading failures, 2) escalating failures, and 3) common cause failures.

- *Cascading failures* occur when a disruption in one infrastructure causes the failure of one or more component(s) in a second infrastructure.

- *Escalating failures* occur when an existing failure in one infrastructure exacerbates an independent disruption in another infrastructure, increasing its severity or the time for recovery and restoration from this failure.

- *Common cause failures* occur when two or more infrastructures are affected simultaneously because of some common cause.

Besides analyzing the types of failures, it is important to understand the different causes that might lead to the occurrence of such failures. As discussed in [Avizienis *et al.* 2004], faults and their sources are very diverse. They can be classified according to different criteria: the phase of creation (development *vs.* operational faults), the system boundaries (internal *vs.* external faults), their phenomenological cause (natural *vs.* human-made faults), the dimension (hardware *vs.* software faults), the persistence (permanent *vs.* transient faults),

the objective of the developer or the humans interacting with the system (malicious *vs.* nonmalicious faults), their intent (deliberate *vs.* non-deliberate faults), or their capability (accidental *vs.* incompetence faults).

Considering the case of electricity infrastructures, historically, attention has been mainly focussed on nonmalicious faults caused by physical (hardware) phenomena or by human-made faults. However, the recent evolution of the electric energy architectures, due to the new economic and organizational models of national deregulated energy markets, with the migration from isolated power utility information systems towards inter and intra connected ICT systems, highlighted the need to focus attention as well on the cyber threats and malicious faults. Malicious faults (such as intrusions, Trojan horses, logic or timing bombs, viruses, worms or zombies) are generally introduced with the objective to alter the functioning of the system during use by: 1) disrupting or halting service, causing denials of service; 2) accessing confidential information; or 3) improperly modifying the system.

Figure 2, including data from [Gao 2004, Schainker *et al.* 2006] and other sources, reports some incidents and attacks that affected electricity and other critical utilities during the last decade. It is noteworthy that a due to the high sensitivity of such data, a complete historical data base of these events is not publicly available (and probably it will never be in the future). Nevertheless, these examples show that the threat is real and it will be increasing due to market deregulation and the increased complexity and openness of the future ICT architectures for power infrastructures. This is confirmed also by the results of the study from the University of British Columbia reported in [Rahman & Besnosov 2006] concerning the identification of sources of failures and their propagation in critical infrastructures, based on public domain reports covering a 12 year period between 1994 and 2005.

Actually, several working groups and initiatives dedicated to the analysis and assessment of security related vulnerabilities and threats in the context of power system infrastructures and the proposal of appropriate solutions to mitigate them have been created recently. A review of emerging standards addressing these issues is presented in [Dondossola *et al.* 2004].

Year	Reported successful cyber attacks
1994	Salt River Project: A water facility in Arizona was breached by a cyber attack. The hacker trespassed in critical areas that could have caused significant damage.
1997	A teenager remotely disabled part of the public switching network in Massachusetts, which shutdown telephone service to 600 customers.
2000	A disgruntled employee of an Australian company used his laptop car computer to remotely hack into the controls of a sewage treatment system, which caused 264,000 gallons of raw sewage to be released into public waterways of Australia over a period of two months. This caused marine life to die and creek water to turn black, producing an unbearable stench to nearby residents, among other impacts.
2000	On October 13, the Control System of Ertan Hydro Station received unexpected signals, then they reduced generation 900MW within 7 seconds, almost causing Sichuan power system to collapse.
2001	Hackers attacked the California Independent System Operator managing the electricity supply of California. The *Los Angeles Times* reported that the cyber hackers "got close" to disrupting power flow during the California rolling blackouts in May 2001.
2001	October 1, many Fault Recorders dysfunctions were caused by a *Timer Logical Bomb*, this type of device had been installed on 146 sets in China
2003	The *SQL Slammer worm* infected and disabled internal systems at a nuclear power plant in Ohio. Safety was never compromised, but a safety parameter display system and the plant process control computer were knocked off-line by the cyber worm for several hours.
2003	On December 30, several *viruses* were found in the control systems of 3 HVDC convert stations (Longquan, Zhengping, Ercheng), which transfer total 6000 MW from Three Gorge to East and South of China
2006	May 18/17/15 --Malware Infection Leaks Japanese Power Plant Data A *malware infection* has being blamed for the leak of sensitive Japanese power plant information onto the Internet. The information included key facility location and operation procedures for the Chubu Electric Power Company's thermal power plant in Owase, Mie Prefecture; some employee data were also compromised. A sub-contractor's use of file sharing software is suspected to have caused the malware infection.

Figure 2: Chronology of reported cyber attacks on electric and other utilities

2.1.4 Service modes and operation states

In order to analyse the dependability of interdependent infrastructures, it is necessary to understand how the different infrastructures depend on each other taking into account the different operation states of each infrastructure that are relevant to the analysis. An infrastructure generally features several performance levels and thus, several modes of service can be distinguished, ranging from full capacity to emergency situation. Actually, these modes of service depend on the workload and level of stress of the system, the different error and failure conditions that might occur and their severity, and the error recovery and restoration actions that can be applied to cope with these failures.

Considering the case of power systems, several theories and models on power systems operating conditions have been published in the literature (see e.g., the summary provided in [Fink & Carlsen 1978, Amin 2005]). A power system is generally characterized as having multiple states or "modes", during which specific operational and control actions are taking place. For example the model in Figure 3 proposed in [Fink & Carlsen 1978][1], distinguished five states: 1) Normal, 2) Alert, 3) Emergency, 4) In Extremis and 5) Restorative.

[1] This model is also used in WP1 for the description of control scenarios (See deliverable D2)

In the *Normal state*, all constraints are satisfied, indicating that the power generation is adequate to supply the existing total load demand, and that no equipment is being overloaded. In this state reserve margins (for power transmission as well as for power generation) are sufficient to provide an adequate level of power with respect to the level of stress to which the system may be subjected. If this level falls below some threshold, or if the probability of disturbance increases, then the system enters the *Alert* state. In this state, preventive actions can be taken to restore the system to the normal state. If a sufficiently severe disturbance takes place before such preventive actions can be applied, the system enters the *Emergency* state. In this state, emergency control actions could be initiated in order to restore the system to at least the Alert state. If these measures are not taken in time, or are ineffective, and if the initiating disturbance is severe enough to overstress the system, then system islanding might occur leading the system to the *In Extremis* State where major portions of the system load would be lost. In this state, load shedding and controlled islanding actions would be needed to prevent total system collapse. Once the collapse had been halted, the system could enter the Restorative state to restore all lost load and reconnect the system. Then, the system could move either to the Alert state or to the Normal state depending on circumstances.

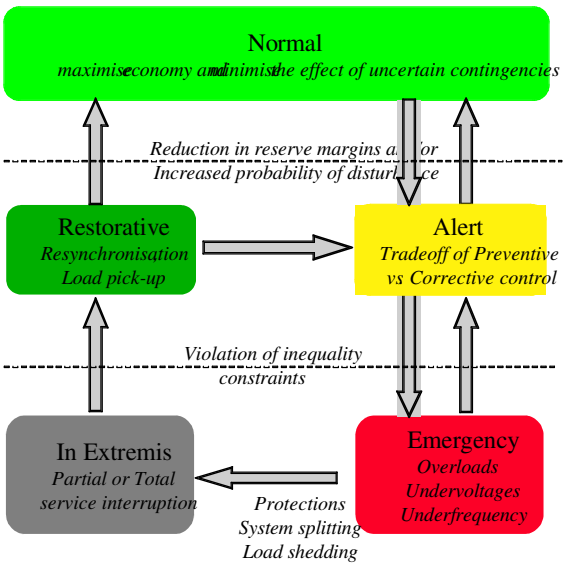


Figure 3: Power system state model (source [Fink & Carlsen 1978])

This example illustrates the need to take into account the progressive degradation of the power systems capability to achieve the expected level of service due to the accumulation of failures, in the electricity infrastructure or the information and control infrastructure, and the ineffective application of restoration and control actions.

2.2 Modelling objectives and challenges

This section summarizes several challenges that need to be addressed when dealing with the modelling of interdependencies and the evaluation of their impact on the dependability of the studied infrastructures. These challenges are directly related to the critical issues identified in Section 2.1 and the multiple dimensions that need to be considered for analysing interdependencies.

There is a wide consensus that developing comprehensive modelling frameworks for understanding interdependencies among critical infrastructures and analysing their impact is a necessary step for building largely interconnected infrastructures on which a justified level of confidence can be placed with respect to their robustness to potential vulnerabilities and disruptions. Modelling can provide useful insights into of how components 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.

Two complementary methods can be used:

- *Qualitative analysis* methods aimed at the identification of failure scenarios, the analysis of their impact and their ranking according to severity and criticality criteria.

- *Quantitative evaluation* methods based on stochastic processes aimed at quantifying the impact of failure and recovery scenarios on the behaviour of the infrastructures and the dependability and trustworthiness of the delivered service. Both analytical and simulation model-based techniques can be used.

Model-based techniques are well suited to support the dependability analysis of systems taking into account various failure and recovery scenarios. In particular, the modelling and comparative analysis of alternative architectural solutions is useful to identify design bottlenecks and select the fault tolerance and maintenance strategies providing the best tradeoffs from the dependability point of view.

There has been extensive work on the modelling of individual infrastructures and various methods and tools have been developed to predict the consequences of potential disruptions within an individual infrastructure. However, the modelling and evaluation of interdependent infrastructures is still at an exploratory stage.

The modelling framework that will be explored during the project is aimed at addressing the multiple dimensions of interdependencies described in Section 2.1, taking into account in particular on: a) the three types of failures that are characteristic of interdependent infrastructures (cascading, escalating, 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 infrastructure investigated. This raises a number of challenging issues from the modelling point of view that are outlined in the following.

Modelling interdependencies related failures. Although the modelling of cascading and escalating failures has received increasing interest in the last years after the large blackouts of electric power transmission systems in 1996 and 2003, this problem is still open and further developments are needed to model such failures and analyse how they contribute to blackouts. The analysis of such types of failures requires the use of models that are able to describe stochastic dependencies and to take into account non-stationary phenomena that result for example from the combined impact of component failures and performance degradations due to overloads. In this case, exponential distributions and Markov modelling may not be appropriate. Hence the need to explore non-Markovian models that are more suited to deal with non stationary phenomena.

Addressing complexity and scalability. A major difficulty in the project lies in the complexity of the modelled 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 will be necessary. The aim is therefore to produce, from conceptual analyses, generic models that can be refined, instantiated and composed according to hierarchical modelling approaches. Resorting to a hierarchical approach brings benefits under several aspects, among which: i) facilitating the construction of models; ii) speeding up their solution; iii) favouring scalability; iv) mastering complexity by handling smaller models through hiding at one hierarchical level some

modelling details of the lower one. Important issues are how to abstract all the relevant information of one level to the upper one and how to compose the derived abstract models. Also, composition rules should be defined to build the models describing each level of the hierarchy from the integration of small generic building blocks describing the models components and their interactions.

Integrated modelling of accidental and malicious threats. Another difficult issue that needs to be addressed when dealing with the resilience assessment of interdependent infrastructures concerns the evaluation of the impact of malicious threats. Traditionally, only accidental faults in software and hardware components have been taken into account in the evaluation of quantitative dependability measures. On the other hand the evaluation of security has been mainly based on qualitative evaluation criteria. Such criteria are widely recognized to be insufficient for analyzing and assessing the impact of malicious attacks and vulnerabilities on the security of systems in operation, or to support the design of intrusion-tolerant systems. The definition of a quantitative evaluation approach based on probabilistic modelling is a promising research direction aimed at filling this gap. The ultimate objective that will be pursued during the project on this topic will be the definition of a comprehensive framework for the modelling and evaluation of resiliency taking into account malicious threats as well as accidental faults.

Modelling of different time scales and phases. Another relevant issue that needs to be carefully addressed in the modelling concerns the description of scenarios that involve variables with different orders of magnitudes leading to the well known stiffness problem. Such a problem can be alleviated by the use of hierarchical modelling and aggregation techniques. Also, we need to address the problem of modelling interdependencies in a context where the studied infrastructures have different operation phases and regimes with different configurations and behaviours. Such changes might have a significant impact on the parameters describing the occurrence of failures and their propagation.

Hybrid modelling of discrete and continuous variables. The characterization of interdependencies between infrastructures and the description of the system dynamics might lead to the need to combine into a single modelling framework continuous and discrete variables. This typically happens when we need to explicitly model the transitions between system operation states as a function of the time variation of some continuous variables that characterize the system dynamics (i.e., transition occurs when the values of some variables exceed some acceptable limits). The approach to this problem can be based on hybrid automata or fluid stochastic Petri nets.

Combination of heterogeneous models and formalisms. An additional line of complexity will raise from the potential need of combining different formalisms to describe the various components of a system and their dependencies, as well as extension of existing formalisms to deal with peculiar features raising from our application context, such as the finite support of stochastic distribution necessary to deal with real-time aspects, the non determinism to describe and verify randomized distributed protocols that could be used in future architectures, and interval mathematics to deal with only partially defined system parameters.

3 STATE OF KNOWLEDGE

This section reviews existing modelling approaches, techniques and tools that can be useful to address the challenges reported in Section 2, and summarizes related work and cooperative projects dealing with the modelling and evaluation of interdependent critical infrastructures in general, and power system infrastructures, in particular.

3.1 Model-based evaluation methodologies and tools

Dependability evaluation based on analytical modelling requires the description of the failure and repair behaviour of system components taking into account various interactions between them. The complexity of the models depends on the dependability measures to be evaluated, the modelling level of detail, and the stochastic dependencies among the components.

Section 3.1.1 presents the model types used for the analysis of stochastic systems. Some examples of modelling approaches that have been developed during the past 15 years to master the largeness of state-space models, based in particular on stochastic Petri nets and their extensions, are reviewed in Section 3.1.2. Section 3.1.3 gives an overview on the available tools that can support the dependability evaluation activity, focusing in particular on the multi-formalism/multi-solution tools. As described in Section 2.2, the quantitative evaluation activity inside CRUTIAL involves several challenges strictly related to the system characteristics, like: a) the need to cope with the complexity of the target infrastructures (scalability problem), b) the need to address continuous and discrete phenomena (that leads to the definition of heterogeneous models) and c) the presence of accidental and malicious threats. A survey of the existing literature dealing with such types of issues is addressed in the last part of the Section. In particular, Section 3.1.4. outlines some of the traditional and emerging approaches focussing on the analysis of the dependability and vulnerability of interconnected systems described as a graph, using network models. Section 3.1.5 deals with the existing heterogeneous modelling approaches, and finally Section 3.1.6 discusses the available modelling and evaluation techniques with respect to malicious threats.

3.1.1 Model types

Model types used in the analysis of stochastic systems can be divided in three broad categories:

1) combinatorial models,
2) models with conditional local dependencies (belief networks)
3) and state-space based models.

In the sequel, we provide a short overview of the modelling formalisms and techniques corresponding to these categories and combined models of different categories.

3.1.1.1 Combinatorial models

Combinatorial models like reliability block diagrams, fault trees and reliability graphs are easy to use and allow for concise system description and inexpensive solution methods. However, a major drawback of these techniques is that they rely on the assumption of independence among components failures and repairs. Such assumption is not always reasonable as different kinds of dependencies can arise in dependability modelling of complex systems [Kanoun & Borrel 2000]: functional, structural, related to the fault tolerance strategies, the maintenance policies, the system mission phase, or the correlation between the system failure behaviour and its workload and performance characteristics.

Among combinatorial models, fault trees have become very popular in the dependability analysis of large safety-critical systems. The goal of fault trees is to represent the combination of elementary causes that lead to the occurrence of an undesired catastrophic event (the top event). The main restrictive assumptions in fault trees are: i) components are modelled as binary objects (up and down); ii) components are statistically independent; iii) interactions are described by means of boolean AND/OR gates (even if extensions of the formalism to NOT and related gates are available).

In order to improve the fault trees modelling power, several extensions to the fault trees formalism were proposed in the literature; we mention Dynamic Fault Trees (DFT) [Bechta-Dugan *et al.* 1992], Parametric Fault Trees (PFT) [Bobbio *et al.* 2003] and Repairable Fault Trees (RFT) [Codetta Raiteri *et al.* 2004]. In DFT, the addition of dynamic gates allows the modelling of dependencies between the events and the component states. In PFT, redundancies and symmetries in the system can be modelled in a compact (parametric) way. In RFT the use of a modelling primitive called repair box is aimed at the modelling of repair processes. In each case, the addition of new modelling primitives requires the study of new solution methods. In particular, DFT and RFT need the state space based solution instead of the BDD (Binary Decision Diagrams) based combinatorial solution applied to fault trees and PFT.

In [Bobbio & Codetta Raiteri 2004], DFT, PFT and RFT formalisms have been integrated in a unique formalism: DRPFT. The analysis of DRPFT models consists of the use of both the combinatorial solution and the state space based analysis and a software framework for the quantitative analysis of DRPFT has been set up. The quantitative analysis of DRPFT typically requires to locate minimal modules of non-independent subtrees of the fault tree and to expand the minimal modules into their state space.

The modelling possibilities offered by fault trees can be extended by relying on Bayesian Networks (BN) [Bobbio *et al.* 2001]. With BN, some constraints that are typical of fault trees can be relaxed, such as the hypothesis that elementary events are always modelled as binary objects (working/failed), are probabilistically independent, and interact just through Boolean AND/OR connections. In [Bobbio *et al.* 2001], it has been shown how fault trees can be directly mapped into BN, and that the basic inference techniques on the latter may be used to obtain classical parameters computed from the former. In addition, local dependencies can be represented and both predictive and diagnostic reasoning can be performed. In [Montani *et al.* 2005] it is shown how BNs can provide a unified framework in which also DFT can be represented.

3.1.1.2 Belief networks

Belief Networks (or Bayesian Networks - BN) have become a widely used formalism for representing uncertain knowledge in probabilistic systems and have been applied to a variety of real-world problems [Heckermann *et al.* 1995]. The main feature of BN is that it is possible to include local conditional dependencies, by directly specifying the causes that influence a given effect. BN are defined by a directed acyclic graph in which discrete random variables are assigned to each node, together with the conditional dependence on the parent nodes. Root nodes are nodes with no parents, and marginal prior probabilities are assigned to them. The quantitative analysis of a BN may proceed along two lines. A forward (or predictive) analysis, in which the probability of occurrence of any node of the network is calculated on the basis of the prior probabilities of the root nodes and the conditional dependence of each node. A more standard backward (diagnostic) analysis that concerns the computation of the posterior probability of any given set of variables given some observation (the evidence) represented as instantiation of some of the variables to one of their admissible values. The inclusion of local dependencies in a BN may avoid a complete state-space description, making the formalism an appealing candidate for dependability modelling and analysis of stochastic systems.

3.1.1.3 State-space approaches

State-space approaches rely on the enumeration of the set of meaningful states of the system and on the specification of the possible transitions among them. In principle, since each system state encodes a complete description of the state of each component, the stochastic behaviour of each component may depend on the state of all the other

components. This extreme flexibility is very seldom exploited in practice since it is very rare to encounter applications in which each component changes its stochastic behaviour according to the state of all the other components. Hence, the state space description appears in some cases overspecified with respect to the real modelling needs. Moreover, in order to make state-space approaches analytically feasible, the dynamic behaviour of the system over its state space must be mapped into a suitable stochastic process. If all the transition times are exponentially distributed the system behaviour in time is mapped into a continuous time homogeneous Markov chain.

The main disadvantage of the state space approaches is the well-known state explosion problem, due to the circumstance that the dimension of the state space grows exponentially with the number of parts. Moreover, the direct specification of the infinitesimal generator of the underlying process may be unfeasible due to its huge size, and some intermediate (higher level) specification languages must be appointed for the scope. Higher-level formalisms such as Stochastic Petri Nets (SPNs) and their extensions have been widely recognized as an effective means to facilitate the specification and generation of state-space models, since they: a) allow a compact representation of the behavior of systems involving synchronization, concurrency and conflict phenomena, b) provide some structural verification of the model, and c) can be automatically converted into continuous time Markov chains [Ajmone Marsan *et al.* 1995]. Such characteristics are actually shared by the more general class of SPNs including GSPNs, ESPNs, Stochastic Reward nets, Stochastic Activity Networks, and stochastic well formed nets.

Significant progress has been obtained during the last 15 years for addressing the state explosion problem at the model construction and model solution levels. Examples of modelling approaches aimed at addressing this problem are presented in Section 3.1.2.

3.1.2 Modelling approaches for mastering complex state-space models

There are two general approaches for dealing with the state explosion problem: *largeness avoidance* and *largeness tolerance* [Nicol *et al.* 2004]. Largeness avoidance techniques try to circumvent the generation of large models using for example, state truncation methods [Muppala *et al.* 1992, Chen *et al.* 2002], state lumping techniques [Kemeny & Snell 1959, Buchholz 1994, Obal 1998, Derisavi *et al.* 2003], hierarchical model solution methods [Buchholz 1995c, Lanus *et al.* 2003], model decomposition and approximate solution techniques [Courtois 1977, Bobbio & Trivedi 1986, Buchholz 1995c, Lanus *et al.* 2003, Daly *et al.* 2004], etc.

However, these techniques may not be sufficient as the resulting model may still be large. Thus, largeness tolerance techniques are needed to provide practical modelling support to facilitate the generation of large state-space models through the use of structured model composition approaches. The basic idea is to build the system model from the composition of submodels describing system components and their interactions. Generic rules are defined for the elaboration of the submodels and their interconnection. Usually, higher-level modelling formalisms such as SPNs and their extensions, are used to support these approaches and generate automatically the Markov chain.

It is worth noting that the two categories of techniques (largeness avoidance and largeness tolerance) are complementary and, most of the time, both of them are used when detailed and large dependability models need to be generated and processed, putting more emphasis on one or the other. For example, even though largeness avoidance, in the sense that the whole system model is not generated and processing is performed on the sub-models, is not the prime concern of largeness tolerance techniques, state-space reduction constitutes a real concern. Generally, in most of the largeness tolerance techniques, rules for model generation are also defined in such a way that they generate the less superfluous states by construction. On the other hand, largeness avoidance relying for instance on the truncation

of the least important states (i.e., states with very small probabilities) can be used to complement efficiently largeness tolerance techniques as in [Muppala et al. 1992]. As other examples of work combining largeness avoidance and largeness tolerance techniques, we can mention [Haddad & Moreaux 1995, Haddad & Moreaux 1996, Delamare *et al.* 2003] which combine sub-model state lumping and Kronecker based continuous time Markov chain representation and solution for models obtained by synchronous or asynchronous composition of (lumpable) submodels (see Section 3.1.2.3).

In the following, we present a survey of modelling approaches based on largeness tolerance and largeness avoidance techniques that can be profitably used in CRUTIAL. Section 3.1.2.1 focuses on compositional approaches based in particular on stochastic Petri nets and their extensions. An overview of the existing works generating stochastic models from High-level design descriptions is presented in Section 3.1.2.2. Section 3.1.2.3 outlines related work dealing with largeness avoidance techniques based on decomposition/aggregation approaches. Finally, Section 3.1.2.4 presents some efficient techniques that can be used to cope with large models at the solution level.

3.1.2.1 Compositional modelling approaches

Several model composition techniques have been developed to support the systematic construction and validation of state-based models characterizing the dependability of large systems involving multiple interactions and dependencies between their components. In addition, model composition is very helpful in supporting models reuse. A brief overview is presented in the sequel.

Research on process algebra [Milner 1989] has inspired efforts to introduce compositionality into Petri nets. Composition of Petri Net consists in constructing PN models from a set of building blocks by applying *suitable* operators of places and/or transition superposition. An example is the Box-calculus approach presented in [Best *et al.* 1992] where composition operators for un-timed Petri Nets are defined, like operators for synchronous/asynchronous communication. Compositionality approaches have been also investigated for stochastic extensions of Petri nets. For example, [Buchholz 1995a] explored composition in the context of SPNs. The work presented in [Donatelli & Franceschinis 1996] proposes a systematic approach to the construction of parallel hardware-software models through the definition of three Generalized Stochastic Petri Net (GSPN) model levels (the process level, the service level and the resource level) and of composition rules to combine them into a complete integrated GSPN model of the whole system. The GSPN composition rules are based on the concept of *matching labels*, that is transitions and places of a GSPN are labelled and pairs of transitions (or places) with matching labels, each one belonging to a different operand, i.e., GSPN component, are superposed.

[Rojas 1996, Ballarini *et al.* 2000] defined a complete set of composition operators for the generation of Stochastic Well-formed Nets (SWN) of a system, (i.e., GSPNs permitting the identification of symmetry by means of a symmetric reachability graph) from the SWN of its components. These operators preserve the functional structure of the model and support several types of communications between components. This approach is intended to support the modelling of distributed and parallel systems where both synchronous and asynchronous communications are required. However, it addresses only a class of systems that can be modelled by SWN.

Compositional modelling is also used in the context of Stochastic Activity Networks (SAN). In [Meyer & Sanders 1993], two composition operators are defined (*join* and *replicate*) to compose system models based on SANs. The Join operator takes as input a) a set of sub-models and b) some shared places belonging to different sub-models of the set, and provides as output a new model that comprehends all the joined sub-models elements (places, arcs, activities) but with the shared places merged in a unique one. The Replicate

operator combines multiple identical copies of a sub-model, which are called replicates. [Obal 1998] introduces a graph composition approach that extends the replicate/join formalism and also combines models by sharing a portion of the state of each sub-model, reducing the total state-space size. Contrarily to the replicate/join formalism that requires the use of a special operation, the graph composition detects all the symmetries exposed at the composition level and uses them to reduce the underlying state space.

The composition techniques discussed above are very helpful to cope with the models complexity, in particular when the models exhibit symmetries. However, they are not sufficient in particular when the modelled systems exhibit various dependencies that need to be explicitly described in the dependability models. These dependencies may result from functional or structural interactions between the components or from interactions due to global system fault-tolerance, reconfiguration and maintenance strategies. Various modelling approaches have been proposed to facilitate the construction of large dependability models taking into account such dependencies. Examples of such modelling approaches are briefly discussed in the sequel.

The block modelling approach defined in [Kanoun & Borrel 2000] provides a generic framework for the dependability modelling of hardware and software fault-tolerant systems based on GSPNs. The proposed approach is modular: generic GSPN submodels are defined to describe the behaviour of the system components and of the interactions between them. The system model is obtained by composition of these GSPNs. The GSPNs of the components and interactions are called block nets. Composition rules are defined and formalised through the identification of the interfaces between the component and interaction block nets. In addition to modularity, the formalism brings flexibility and re-usability thereby allowing for easy sensitivity analysis with respect to the assumptions that could be made about the behaviour of the components and the resulting interactions. The main advantage of this modelling approach lies in its efficiency for modelling several alternatives for the same system as illustrated for example in [Kanoun *et al.* 1999].

The efficiency of the block modelling approach can be further improved by using an incremental and iterative approach for the construction and validation of the models as suggested in [Fota *et al.* 1999]. At the initial iteration, the behaviour of the system is described taking into account the failures and recovery actions of only one selected component, assuming that the others are in an operational nominal state. Dependencies between components are taken into account progressively at the following iterations of the modelling process. At each iteration, a new component is added and the GSPN model is updated by taking into account the impact of the additional assumptions on the behaviour of the components that have been already included in the model. Similarly to the block modelling approach, sub-models are defined for describing the components behaviours and specific rules and guidelines are defined for interconnecting the submodels taking into account their interactions.

An iterative dependability modelling approach has been also proposed in [Betous-Almeida & Kanoun 2004a] where the construction and validation of the GSPN dependability model is carried out progressively following the system development refinement process, to facilitate the integration of dependability modelling activities in the system engineering process. Three main steps are distinguished. The first step is dedicated to the construction of a functional-level model describing the system functions, their states and their interdependencies. In the second step, the functional level model is transformed into a high-level dependability model based on the knowledge of the system's structure. A model is generated for each pre-selected candidate architecture. The third step is dedicated to the refinement of the high-level dependability model into a detailed dependability model for each selected architecture. Formal rules are defined to make the successive model transformations and refinements as easy and systematic as possible taking into account three complementary aspects: i) component decomposition, ii) state/event fine-tuning, and iii) stochastic distribution adjustments. This approach allows the integration of various dependencies at the right level

of abstraction: functional dependency, structural dependency and those induced by non-exponential distributions. A case study is described in [Betous-Almeida & Kanoun 2004b].

Actually, the approach presented in [Betous-Almeida & Kanoun 2004a] can be seen as a special case of the more general class of techniques based on layered and multi-level modelling methods, where the modelled system is structured into different levels corresponding to different abstraction layers, with a model associated to each level. Various modelling approaches based on this idea have been proposed in the literature, see e.g., [Donatelli & Franceschinis 1996, Bondavalli *et al.* 2001, Bernardi 2003, Bernardi & Donatelli 2003, Kaâniche *et al.* 2003, Rabah & Kanoun 2003, Lollini *et al.* 2005]. For example, the multilevel modelling approach proposed in [Kaâniche *et al.* 2003] for evaluating the user perceived availability of web-based applications distinguishes four abstraction levels, namely, user, function, service and resource levels. The highest level (user level) describes the availability of the application as perceived by the users. Intermediate levels describe the availability of functions and services provided to the users. The lowest level (resource level) describes the availability of the component systems on which functions and services are implemented. Another example is the PSR layered approach originally presented in [Donatelli & Franceschinis 1996] and then extended to dependability aspects in [Bernardi 2003, Bernardi & Donatelli 2003] which structures the system into three levels: 1) resources, 2) services, and 3) processes. Resources are at the bottom level and they provide operations for the services, where a service is basically a complex pattern of use of the resources. Services are then requested by the application model placed at the highest level, called process level. This approach has been used in the context of the DepAUDE project for modelling the dependability of automation systems.

Generally, layered and multilevel modelling approaches rely on the hierarchical composition and solution of the submodels corresponding to the different abstraction levels. Different modelling techniques can be used to describe the submodels and to combine their results (combinatorial models, state-based models). The selection of the right technique mainly depends on the kind of dependencies between the elements of the corresponding submodels and on the quantitative measures to be evaluated. It is noteworthy that hierarchical modelling approaches combining different types of models are supported automatic tools, e.g., SHARPE modelling tool [Sahner & Trivedi 1987][Sahner *et al.* 1996] (see Section 3.1.3 for an overview of modelling tools). These approaches belong to the more general class of model decomposition and aggregation approaches presented in Section 3.1.2.2. Some application examples of hierarchical modelling and solution are also presented in this section.

3.1.2.2 Overview of decomposition/aggregation modelling approaches

In this Section we focus the attention on the decomposition/aggregation modelling approaches, that is a type of largeness avoidance technique that tries to circumvent the generation of large models using model decomposition and aggregation of the partial results. The basic idea is the following: the overall model is decoupled in simpler and more tractable sub-models, and the measures obtained from the solution of the sub-models are then aggregated to compute those concerning the overall model.

Among the existing works adopting a decomposition/aggregation approach, in the following we select some of them focusing on those that could be more profitably applied to deal with CRUTIAL challenges like largeness, multiplicity of interactions and types of interdependencies involved, models stiffness, the need to describe multiple phases with different characteristics, including some works proposed by CRUTIAL partners.

The proposed decomposition and aggregation techniques depend on the type of measures to be evaluated (steady-state or transient) and the modelling formalism. Generally

approximate solutions are provided for the composition of the results derived from the submodels.

A decomposition and aggregation theory for steady state analysis of general continuous time Markov Chains has been proposed in [Courtois 1977]. The quality of the approximation is related to the degree of coupling among the blocks into which the Markov chain matrix is decomposed. In [Bobbio & Trivedi 1986] the authors present an extension of this technique specifically addressed to the transient analysis of large stiff Markov chains, where stiffness is caused by the simultaneous presence of “fast” and “slow” rates in the transition rate matrix. The set of all states is classified into fast and slow states, and an algorithm proceeds by further classifying fast states into fast recurrent subsets and a fast transient subset. The fast subsets are separately analyzed, and each fast recurrent subset is replaced by a single slow state while the fast transient subset is replaced by a probabilistic switch. The resulting Markov chain is small and non-stiff, and then it can be solved using standard techniques. The results produced by the algorithm are asymptotically exact with respect to the aggregation of fast transient states, while the asymptotic accuracy for fast recurrent subsets depends on the degree of coupling between the fast subset and the remaining states.

The key idea of time-scale based decomposition has been applied to Non-Markovian stochastic systems as in [Haddad & Moreaux 2004], and also to GSPN models of systems containing activities whose durations differ by several orders of magnitude. For example, In [Ammar & Rezaul Islam 1989] the given GSPN model is decomposed into a hierarchical sequence of aggregated sub-nets each of which is characterized by a certain time scale. Then these smaller sub-nets are solved in isolation, and their solutions are combined to get the solution of the whole system. The aggregation at each level is done by assuming that the transitions included in the lower level are immediate transitions. At each level of the hierarchy, the current marking of an aggregated sub-net determines the number of tokens in the sub-net at the lower level, which are then analyzed to determine the rate of transitions in the aggregated sub-net.

Another interesting extension of the decomposability theory presented in [Courtois 1977] is the decomposition approach for the solution of large stochastic reward net models proposed in [Ciardo & Trivedi 1993]. In this work the overall model consists of a set of submodels whose interactions are described by an import graph; each node of the graph corresponds to a parameterized stochastic reward net submodel and an arc from submodel A to submodel B corresponds to a parameter value that B must receive from A. The authors show that the probability that a subnet is in a state satisfying a given condition, the average time a given condition remains satisfied, and the expected time until the subnet satisfies a given condition are three quantities that suffice for intercommunication among subnets for the net structure types that they define.

The decomposition approach proposed by [Daly 2001, Daly & Sanders 2001] is based on a new set of connection formalisms that reduce state-space size and solution time by identifying submodels that are not affected by the rest of a model, and solving them separately. The result from each solved submodel is then used in the solution of the rest of the model. The authors develop four abstractions that can be used to make connection models, and they involve passing a continuous-time random process, a discrete-time random process, a random variable, and an average value between the models. When these abstractions are applied, each submodel should have a smaller state space and fewer time scales than the complete model.

Decomposition approaches are also relevant for the modelling of multiphased systems. In CRUTIAL, the studied infrastructures have different operation phases and regimes with different configurations and behaviours, and such changes might have a significant impact on the parameters describing the occurrence of failures and their propagation within an infrastructure or between different infrastructures (interdependencies). Therefore, one research direction will be to investigate the use of stochastic models for multi-phased

systems. In the literature, several approaches have been proposed for the analytical dependability modelling of Phased Mission Systems (PMS), all based on a hierarchical structure of the models. PMS are characterized by a sequence of phases in which the system configuration can change during operations. The existence of phases is a consequence of: i) diverse tasks to be performed, and ii) diverse environmental conditions, in different periods of system lifetime.

In [Bondavalli *et al.* 1999b, Mura *et al.* 1999], the model of a PMS is seen as composed of two logically separate Petri nets: the System Net (SN), representing the system (its components, their interactions and their failure/repair behaviour) as a GSPN, and the Phase Net (PhN), a deterministic and Stochastic Petri Net - DSPN, representing the control part and describing the phase changes. In the SN, a single model is built for the whole mission, characterized by a set of phases without detailing the behaviour of the system inside each phase. This allows easy modelling of a variety of mission scenarios by sequencing the phases in appropriate ways. The parameter values to be used in the SN model are obtained by solving the PhN models. This approach has been generalized in [Mura & Bondavalli 2001] in which the authors proposed a new methodology based on a Markov Regenerative Stochastic Petri Nets (MRSPN) approach. The key point is that the state space of the Markov regenerative process is never generated and handled as a whole, but rather the various subordinate intra-phase processes are separately generated and solved. As a consequence, the computational complexity of the analytical solution is reduced to the one needed for the separate solution of the different phases, as demonstrated in [Bondavalli & Filippini 2004].

In [Lollini 2005] it is proposed a decomposition/aggregation approach that operates at the system-level, rather than the model level. Using this approach, “entities” (or sub-systems) are created that can work in isolation or can interact with each other through a set of “dependency relations”. The relations state how the behaviour of each entity affects the others. The structure, together with the notion of a phased mission, allows one to solve each submodel in isolation, and then pass results between submodels as needed. Such formulation can be applied to many models, and reduces the complexity of solving models that can be expressed in this framework. This generic decomposition/aggregation approach has been applied to study a GPRS mobile telephone infrastructure that takes into account the congestion that can occur following service outages and the subsequent impact of this congestion on user-perceived quality of service.

The approach introduced in [Balakrishnan & Trivedi 1995] is aimed at solving reliability models for systems with repairable components. A submodel is built for each component, and the reliability of the whole system is derived from the sub-model solutions. The sub-model for a given component must contain system-state information to ensure that the repair process is active only for the system up states. A natural construction procedure is to identify if the component in question is up or down, and to augment the sub-model with the system up/down information. This leads to a four-state sub-model having two absorbing states. Each sub-model state is an aggregate of system states. Three examples illustrating this approach have been presented, including n-Component parallel redundant systems and n-component systems with general structure.

The technique presented in [Woodside *et al.* 1995] has been developed for the modelling of synchronous distributed software using Stochastic Rendezvous Networks (SRNs). SRNs consist of tasks that take a random amount of time and may require the services of other tasks in order to complete. In [Woodside *et al.* 1995], a logical decomposition modelling approach has been presented for SRNs: each task is modelled separately, with the dependencies between tasks specified, and the tasks communicate by messages in a request-wait-reply sequence (which models a ‘rendezvous’). Queueing and synchronization involving inter-task messages are implicit in the SRN framework, so a given model can be stated much more compactly with respect to Petri nets.

A modular and hierarchical decomposition modelling approach applied to a railway interlocking system has been defined in [Nelli *et al.* 1996, Bondavalli *et al.* 2001]. The system is modelled at the various levels of the hierarchy, and each layer has been structured for producing some results while hiding implementation details and internal characteristics. Then the output values from one layer are used as parameters of the next higher layer, and the different layers can be modelled using different tools and methodologies.

Finally, in [Lollini *et al.* 2005], a dependability analysis for a class of hierarchical control systems has been carried out. The functionalities of the whole system are partitioned among a number of subsystems working at different levels of a hierarchy, and the dependability of the whole system is enhanced considering, at each level, both internal checks and interface checks. A proper modelling methodology based on a decomposition approach has been defined, able to reduce the system complexity. They first decompose a model starting from its functional specification and applying a stepwise refinement to decompose it in small sub-models. Then, modular model solution is carried out in a bottom-up fashion.

3.1.2.3 Derivation of dependability models from high-level specifications

Besides the modelling approaches presented in the previous sections that are aimed at mastering the complexity of dependability models at the state level or at higher-level model representations such as at the GSPN level, further improvements can be obtained by generating the dependability models from the transformation of design descriptions enriched with dependability related information. The literature presents several approaches to generating performance and dependability models from UML designs and in [Balsamo *et al.* 2004] a survey of the main contributions is presented. Some examples of contributions from CRUTIAL partners are briefly presented in the following.

The work presented in [Bernardi *et al.* 2002] proposes a method that generates a GSPN model from a UML performance annotated design. The UML specification includes state machines (SMs) and sequence diagrams (SDs). The proposed approach exploits GSPNs' compositional features, to master complexity in both defining and implementing the generation process, which consists of three main steps. First, the approach involves translating SMs separately into GSPN models characterized by labelled places and transitions. Labelled places represent mailboxes associated with event types, whereas labelled transitions can represent event generation or event consumption. The second step translates the SD into a GSPN model with labelled transitions, capturing the causal relations between the represented scenario's events as well as the message transmission delays. The last step presents two choices: 1) compose the SM GSPN models over labelled places to produce the performance model of the system, *SysModel*; 2) compose *SysModel* with the SD GSPN model, over labelled SD transitions, to obtain a performance model for a system scenario, *ScenarioModel*. During the translation steps, the performance annotations specified in the UML diagrams are used to define the GSPN model's input parameters.

Although the approach proposed in [Bernardi *et al.* 2002] is not focused on dependability analysis, it has been used for the QoS assessment of fault tolerance strategies of software systems (see [Bernardi & Merseguer 2006], for example), characterized by both performance and dependability requirements.

Other approaches are instead specifically aimed at the dependability assessment of software systems such as [Bondavalli *et al.* 1999a, Bernardi & Donatelli 2003, Majzik *et al.* 2003, Cortelessa & Pompei 2004]. In [Bondavalli *et al.* 1999a, Majzik *et al.* 2003] UML extension mechanisms are proposed for annotating dependability properties of software systems on UML design models. From the annotated models, Petri Net models can be derived to use in the quantitative system evaluation. The nonfunctional properties considered are the reliability and the availability. Dependability parameters, that can be both input parameters or measured to be derived, can be used to characterize the timing occurrence of faults, the

possible error latency for components with an internal state, and the timing of the repair process. Error propagation between components is specified by assigning a probability to the model elements representing either relations or interactions between such components (such as association between software components, communication path between nodes and exchanged messages). While dependability parameters can be used to specify component failures due to independent fault occurrences, common failure modes can be specified only for redundant components belonging to complex fault tolerance structures. Extensions for states and events of state machines representing the behaviour of *redundancy manager* components are introduced in order to discriminate normal and failure states and events. Such extensions are used to analyze different failure modes of the fault tolerance structures.

In [Cortelessa & Pompei 2004] a UML annotation for the reliability analysis of component based systems is defined. The work is aimed at including the annotation approach presented in [Cortelessa *et al.* 2002], where Bayesian models are derived from UML annotated models (Sequence, Communication, Deployment and Use Case diagrams) to compute the system failure probability, within the frameworks of the standard UML profiles.

Finally, the work [Bernardi & Donatelli 2003] considers the problem of building Petri net based evaluation scenarios for dependable automation systems and proposes a modelling process in which as much information as possible is extracted from a high level description of system entities, their relations and its fault tolerance strategies using UML Class diagrams. This preliminary description, which is available at the early stages of the application development, is then completed with operational specifications of system behaviour. The class of nets of reference is that of GSPNs, and their coloured extension Stochastic Well Formed Nets (SWN), so that the system under study can be both validated and evaluated.

Further proposals on extending UML to support dependability analysis of software systems can be found in the recent work [Bernardi & Merseguer 2007], where an extensive review of the literature has been made. Modelling approaches considering other design languages such as AADL are also investigated, see e.g., [Rugina *et al.* 2006].

3.1.2.4 Mastering complexity at the solution level

In addition to the modelling approaches outlined in the previous subsections, and the solution techniques presented in the context of decomposition and aggregation modelling approaches, space and time efficient algorithms have been developed to reduce the storage requirements of the state space and the generator matrix and to optimize the state space exploration, generation and analysis. These model solutions algorithms are generally used in combination with the modelling techniques aimed at mastering complexity at the model construction level. Many of the recent algorithms that have achieved notable success use symbolic data structures like binary or multi-valued decision diagram data structures, matrix diagrams or Kronecker representations (see e.g., [Ciardo & Miner 1999, Buchholz *et al.* 2000, Miner & Parker 2004]).

With Kronecker algebra it is possible to develop efficient solution techniques for continuous time Markov chains that compute the steady state distribution without generating and storing the corresponding infinitesimal generator, Q, explicitly. The idea is to represent Q as a sum of Kronecker products of smaller matrices resulting from a high-level model structured into submodels. The method has been applied to several high-level formalisms where models are described in a compositional way ([Plateau 1985, Donatelli 1993, Donatelli 1994, Kemper 1996, Scarpa & Bobbio 1998]). In [Haddad & Moreaux 1995, Haddad & Moreaux 1996] and [Delamare *et al.* 2003] the decision diagram and Kronecker representations are combined with lumping techniques (for Stochastic Well Formed Nets) for improved efficiency. The method can be applied to a subclass of SWN which covers a relevant number of applications. It is noteworthy that with Kronecker representation one can describe not only large Markov chains but also transition systems [Bobbio & Horváth 2001] and discretization

schemes for a set of differential equations describing fluid stochastic Petri nets [Gribaudo & Horváth 2002].

Since with Kronecker representation, one looks for the solution without explicitly storing the infinitesimal generator, solution methods exploiting a Kronecker structure are iterative. The basic operation either for steady-state or transient analysis is vector-matrix multiplication. There are different ways to carry out this basic operation on a Kronecker structure. A family of solution techniques together with references to others can be found in [Buchholz *et al.* 2000].

Besides providing efficient means for representing the infinitesimal generator of large Markov chains, we need also to address the problem of storing the vector of the solution itself. To overcome this problem, a technique is suggested in [Horváth 2005] which, starting from the Kronecker description, first performs Gaussian elimination of a set of states (resulting in an infinitesimal generator whose explicit storage is not necessary) and then performs an iterative algorithm.

In addition to Kronecker algebra, other techniques can be investigated in the context of CRUTIAL to optimise the solution of complex stochastic models, for example the Flow Equivalent Server (FES) approach and product-form solutions for stochastic Petri nets. The FES approach, also called flow equivalent aggregation, was first introduced in [Chandy *et al.* 1975] for the analysis of queueing networks. The basic idea is to substitute a submodel by a single server that preserves the behaviour of the submodel from some point of view. For this purpose, the submodel is analysed in isolation by taking it off the system, “shorting” its input/output interfaces, (thus making the submodel closed, according to the terminology of the BCMP theorem [Baskett *et al.* 1975]) and varying the number of costumers in the submodel up to the maximum allowed by the whole system. The throughput computed along the short-circuit path for the different subsystem populations is used as the load dependent service rate of the single server that is used to substitute the submodel in the representation of the whole system.

The approach is exact for arbitrarily connected closed queueing networks with product-form solution (i.e. BCMP networks [Baskett *et al.* 1975]) while it can be applied to approximate non-BCMP networks. In general the approach results in good approximations when the behaviour of the subnet depends mainly on the number of its customers and can be assumed to be independent of the arrival process.

Variants of the approach, that set up iteration schemes based on specific application structures, are often used to improve the approximations in some cases; see [Marie 1979, Jacobson & Lazowska 1981] for examples of these methods. The idea of using the FES approach for the solution of non-BCMP networks naturally leads to the application of this method to the analysis of models developed with different modelling formalisms, see [Balbo *et al.* 1986, Jungnitz & Desrochers 1991] for application of FES to Petri nets. A more flexible approach is when the subnet is substituted not by a single server but by a subnet smaller than the original one [Buchholz 1995b].

The FES approach is particularly useful to support the analysis of hierarchical models. However, if the models fall within the category of non-BCMP networks (and this will be probably the case of CRUTIAL models), it will be necessary to carefully validate the accuracy of the results and devise appropriate improvement schemes if needed. The validation could be done by simulation or alternative (more expensive) analytical techniques.

It is noteworthy that similarly to queueing networks, product-form solutions have been explored for computing the steady-state probability distribution of Stochastic Petri Nets (SPNs) from the late 1980’s as an attempt to cope with the state explosion problem for SPN models [Balbo 1995]. In particular, several studies have focussed on the identification of the SPNs properties that are relevant with regard to the existence of a product-form solution. Historically, initial proposals have first explored behavioural properties based on an analysis of the reachability graph as in [Lazar & Robertazzi 1987], and then progressively introduced

more and more structural parameters to ensure a product-form solution as proposed in [Henderson *et al.* 1989][Boucherie 1993][Haddad *et al.* 2005]. A more detailed discussion of these approaches can be found [Haddad *et al.* 2005]. Computational algorithms were also proposed in [Coleman 1993][Sereno & Balbo 1993].

3.1.3 Supporting modelling and solution tools

In this Section we provide a list of available tools that could be profitably used as support for the dependability evaluation activity inside CRUTIAL. As detailed in [Sanders 1999], they can be grouped in two main classes: the single-formalism/multi-solution tools, and the multi-formalism/multi-solution tools.

The **single-formalism/multi-solution tools** are built around a single formalism and one or more solution techniques. They are very useful inside a specific domain, but their major limitation is that all parts of a model must be built in the single formalism supported by the tool. DSPNexpress [Lindemann *et al.* 1999], GreatSPN [Chiola *et al.* 1995, Illié *et al.* 2004], SURF-2 [Béounes *et al.* 1993], DEEM [Bondavalli *et al.* 2000], TimeNET [German *et al.* 1995a], UltraSAN [Sanders *et al.* 1995], and HiQPN [HiQPN] are only some examples of tools based on Stochastic Petri Nets formalism and its extensions. They all provide analytic/numerical solution of a generated state-level representation and, in some cases, support simulation-based solution as well. In particular, GreatSPN tool includes the *algebra* software package that implements the composition of GSPN models as well as of their colored extension (Stochastic Well Formed Net - SWN)[Bernardi *et al.* 2001].

An expected difficulty to be addressed in CRUTIAL is the heterogeneity of the models, given the very different nature of the various components under study. This means that different parts of the system could be modelled using different formalisms and then solved using appropriate solution techniques, also accounting for their interactions. For this reason, inside CRUTIAL the **multi-formalism/multi-solution tools** seems to have greater potentialities than the single-formalism/multi-solution tools, since such tools support multiple modelling formalisms, multiple model solution methods, and several ways to combine the models, also expressed in different formalisms.

With respect to the level of integration between modelling formalisms and solution techniques, we can identify two different sets of tools.

- The first set includes tools that try to unify several different single-formalism modelling tools into a unique software environment (loose integration). Examples are IMSE (Integrated Modelling Support Environment) [Pooley 1991], that is a support environment that contains tools for modelling, workload analysis, and system specification, IDEAS (Integrated Design Environment for Assessment of Computer Systems and Communication Networks) [Fricks *et al.* 1997], that provides a broad range of modelling capabilities without the need to learn multiple interface languages and output formats, and FREUD [van Moorsel & Huang 1998], that focuses on providing a uniform interface to a variety of web-enabled tools.

  A more recent model design framework is the DrawNet Modelling System (DMS) [Franceschinis *et al.* 2002, Codetta Raiteri *et al.* 2006] that supports an Object-Oriented (OO) design process of system models and provides a graphical front-end (the DrawNet GUI) to existing performance tools and a Java library (the DNlib) meant to ease the integration in the DMS of new modelling formalisms and interfaces to existing as well as new solvers. The DMS is based on a set of languages that allow to define modelling formalisms, model classes and model objects. Among its several OO features we cite the inheritance of modelling formalism specifications, that allows the definition of modelling formalism hierarchies: new modelling formalisms are created from existing ones by inheriting their elements (nodes and/or edges), and overriding some of them or extending their properties. In a formalism, several aspects have to be defined, such as

the primitives of the formalism, the measure to be computed on the models, and the graphical representation of the formalism primitives. An XML format has been defined for the concrete storage of formalisms and models. The inheritance mechanism is also the basis for multi-formalism models since it is possible to embed a submodel described with formalism F1 in a model described with formalism F2. Multi-solution is supported by a set of functions in the DNlib, including input/output filters to produce/read solver specific input/output files and solver management functions (to ease the link between a formalism and a solver and provide the solver invocation methods). Complex multi-solution procedures could be supported through a solution process specification language and a solution engine able to execute it, much along the line of what has been proposed in [Gribaudo *et al.* 2005].

- The second set includes tools in which the new formalisms, composition operators and solvers are actually implemented within a unique comprehensive tool (tight integration). Among the existing tools having these characteristics, we cite SHARPE [Trivedi 2002], that is a tool for specifying and analyzing performance, reliability and performability models, SMART [Ciardo & Miner 1996], that is a multi-formalism modelling tool to study complex discrete-state systems, DEDS [Bause *et al.* 1998], that is a toolbox for the construction of modular tools for functional and quantitative analysis of discrete event dynamic systems, and POEMS [Adve *et al.* 2000], that is a tool for modelling complex parallel and distributed systems.

  MÖBIUS [Daly *et al.* 2000] is another important multi-formalism/multi-solution tool. It supports different formalisms like SAN, PEPA, Buckets and Balls, and Fault Tree, as well as the composition of models described using different formalisms. Concerning the solution process, it supports both state-based, analytical/numerical techniques (when applicable) and discrete event simulation (both transient and steady-state, applicable to any model).

3.1.4 Network models

Critical infrastructures can be seen as a complex network of interacting systems and components, and as a consequence can be analyzed using network models theory. Network models have been traditionally used to analyse the dependability and performance of systems described as a graph, taking into account their topology and the failures affecting the nodes and the links interconnecting them.

Complex networks display a high degree of tolerance to random failures, errors and attacks due to the redundant paths that usually connect the vertices. Network reliability is defined as the probability that two specific nodes (a source node and a destination node) are connected given the probability of the elements of the network (nodes, edges or both) of being up or down. A number of techniques have been developed to tackle this problem. However, with the appearance of networks of giant dimensions (e.g., the electric grid, the internet and www) the traditional exhaustive searching techniques are no more appropriate. A completely new field of research has emerged to study the statistical properties of huge networks, together with the study of their robustness to random failures, cascading failures and attacks.

Exhaustive analysis techniques are intended to provide qualitative and quantitative information on the network connectivity, dependability, and vulnerability. A literature survey indicates that the approaches, which have been used to compute two-terminal reliability could broadly be classified into two paradigms [Bobbio *et al.* 2006]:

i) the paradigm in which desired network reliability is directly calculated (series-parallel reduction or pivotal decomposition using keystone components [Page & Perry 1988, Hardy *et al.* 2005],

ii) and the paradigm in which all possibilities through which the two specified nodes can communicate (or not communicate) with each other are first enumerated (path/cut set search [Luo & Trivedi 1998, Balan & Traldi 2003]) and then reliability (unreliability) expression is evaluated. The use of Binary Decision Diagrams (BDD) [Bryant 1986] provides an extraordinarily efficient method to represent complex binary structures and algorithms exploiting the direct use of BDDs to model the network connectivity, and the level of reachable complexity, needs to be investigated more deeply.

However, the complexity of real world today networks (the internet, the www, the public power grid telecommunication networks), can reach millions or even billions of vertices. This change of scale forces a corresponding change in the analytic approach. Many of the approaches that have been applied in small or medium scale networks, and many of the questions that have been answered are simply not feasible in much larger networks. Recent years have witnessed a substantial new movement in network research [Albert & Barabasi 2002b, Dorogovtsev & Mendes 2002, Newman 2003, Boccaletti *et al.* 2006], with the focus shifting away from the analysis of small graphs to consideration of large-scale statistical properties of graphs and with the aim of predicting what the behaviour of complex networked systems will be on the basis of measured structural properties and the local rules governing individual vertices. The shift, experienced in the past few years in the understanding of complex networks, was rapid and unexpected. Empirical studies, models and analytic approaches have enlightened that real networks display generic organizing principles shared by rather different systems. These advances have created a prolific branch of statistical mechanics, followed with equal interest by sociologists, biologists and computer scientists. Moreover, the structural organization of a complex network influences how the system reacts to occasional failures or to intentional attacks [Crucitti *et al.* 2003], and hence has a direct impact on the dependability and security of these structures. Finally, a new area of research refers to the propagation of failures in a complex graph due to avalanche of breakdowns when node and links are sensitive to overloading. In a power transmission grid, for instance, each node (power station) deals with a load of power. The removal of nodes, either by random breakdown or intentional attacks, changes the balance of flows and leads to a global redistribution of loads over all the network that can be, in some cases, not tolerated and might trigger a cascade of overload failures. This problem is usually referred in the literature as cascading failures [Crucitti *et al.* 2004a, Zaho *et al.* 2004]. A more detailed discussion of the state of the art dealing with cascading failure models is presented Section 3.2.1.2.

3.1.5 Heterogeneous models

Among the challenges to be addressed in the context of interdependent critical infrastructure as listed in Section 2.2, we can mention the need: i) to take into account timing constraints, ii) to describe different types of uncertainties concerning the system dynamics and behaviour or nondeterministic choices related to system recovery or fault and intrusion tolerance strategies, iii) to model both discrete and continuous variables, or iv)) to model non exponential distributions. In this subsection we outline potential models in addition to those mentioned in the previous sections, that can be used to address these issues.

A possible categorization of models can be according to the following two main attributes: *i)* the timing specification (stochastic or non-stochastic) and *ii)* the model state space (discrete or continuous or partly discrete and partly continuous). The use of supplementary variables in stochastic models converts a discrete state space with any kind of timed transitions into a partly discrete and partly continuous state space. Hence, the two main categories above can be merged into a single one: heterogeneous models.

3.1.5.1 Timing specification and modelling

In stochastic models the timing of events is represented by means of random variables, and typical fields of application are performance evaluation and reliability analysis. The analysis tools are based on the theory of stochastic processes, and the most commonly exploited form is when all the timed random variables are exponential so that the underlying stochastic process is a continuous time Markov chain (CTMC). The obtainable quantitative measures are in the form of mean values (or more generally speaking moments) and distributions.

In timed models the timing of events is represented by constant values or non-deterministic intervals. Typical fields of application are protocol or program verification and deadline verification in real-time systems. The analysis tools are based on checking the validity of a logical expression (according to some specification semantics) or to find a counter example; the procedure of specifying a formula and finding its validity is known as model checking. The obtainable measures are in the form of reachability properties.

Two formalisms for describing non-stochastic timed models with discrete state space can be considered: *Timed Automata* (TA) [Alur & Dill 1990, Alur & Dill 1994] and *Time Petri Nets* (TPN) [Merlin & Faber 1976].

TA extend classical frameworks for the description of the dynamics of the system, such as automata and transition systems, and are obtained by equipping a finite graph with a finite number of real-valued variables called clocks, which increase at the same rate as real-time. The vertices of the graph correspond to control modes in which the system can be in as time elapses. At certain points in time, the TA can instantaneously traverse an edge from one vertex to another. For any given graph edges, the points in time at which the edge can be traversed depend on the current values of the clocks; this dependency is determined by clock constraints, which are logical formulae on clock values, and which label graph edges. More precisely, the graph is labelled with conditions on clocks, which influence the transitions taken between vertices in the graph: for example, clock constraints labelling edges determine which values clocks must have for the edge to be traversed; similarly, clock constraints labelling vertices determine the values of clocks which, when reached, force the TA to leave the vertex (such constraints may be used to describe the expiration of time-outs or deadlines, for example). We also note that a set of clocks can be reset to 0 on traversal of an edge.

TPN extend the basic model of Petri Nets by adding timing constraints on the execution of transitions [Merlin & Faber 1976, Berthomieu & Diaz 1991, Bucci & Vicario 1995, Berthomieu & Vernadat 2003]. Every transition is associated with a static firing interval, made up of an earliest and a latest firing time. When the transition is first enabled, it is associated with a clock which is maintained until the transition is enabled with continuity. The transition cannot fire before its clock has reached the earliest firing time, neither it can avoid to fire when the clock reaches the latest firing time. In general, the logical sequencing of processes and their mutual dependencies can be conveniently captured in an operational model, such as a finite state machine, a Petri Net, or any kind of automaton. Timing constraints are added to the representation by timers and durations constraining the intervals in which model events are either prevented or forced to execute. TA and TPN are notable examples layering this timing semantics on top of State Transition Systems and Petri Nets, respectively. To encompass preemptive process scheduling, the model must be further extended by associating priorities to events timed activities [Vicario 2001]. In the analysis of a TPN, state space enumeration methods enable verification of properties pertaining both to the logical sequencing of events and to their timing. This approach is basically hurdled by the fact that the state of a TPN depends not only on the marking but also on timers associated with transitions.

The TA and TPN formalisms have a common underlying semantic model, and TAs and bounded TPNs are equivalent in terms of timed, linear-time properties (such as those properties which can be expressed in a linear-time temporal logic). We note that every bounded TPN (that is, a TPN with a finite number of reachable markings) can be translated into an equivalent TPN. Both TA and bounded TPNs may be verified against reachability or

temporal logic properties, which may themselves include timing constraints such as deadlines: for example, the property “a response always follows a request within 0.05 seconds after the request was made”.

3.1.5.2 Markov Decision Processes

In some cases it is necessary to model systems with unknown scheduling mechanisms or with transitions whose next-state probability distribution is not known with precision. A number of models which feature behaviour which can arise from both probabilistic and nondeterministic choices, and which can model such systems, have been presented in the literature; among these formalisms, Markov Decision Processes (MDP) have been widely studied and used in a variety of areas, including verification, planning, robotics, automated control, economics and in manufacturing [Puterman 2005].

MDPs were introduced by Bellman and Howard in [Bellman 1957, Howard 1960] in the context of operations research and dynamic programming, and are an extension of Markov chains (MC). The principal difference is that MDPs make state transitions according to a two-phase choice: the first phase consists of a nondeterministic choice of an action, while the second phase consists of a probabilistic choice according to the probability distribution which is associated to the chosen action in that state. The probabilistic choice in the second phase determines to which state the system then moves. If only one action is possible from each state, or if the action to take is somehow fixed for each state, the MDP reduces to an MC. Thus an MDP represents an infinite number of MCs which we can obtain by defining a probability distribution on the different actions (corresponding to nondeterministic choices) associated with each state. We also note that, for every action in each state, a reward is defined.

MDPs have been used in the context of the verification to model communication protocols and randomized, distributed algorithms, such as the Root Contention protocol of the IEEE 1394 (FireWire) standard [Kwiatkowska & Sproston 2003]. In the context of studies of electricity supply, MDPs have been used to analyze bidding strategies [Song *et al.* 2000]. We note that MDPs are a low-level system-description formalism, and therefore higher-level languages are used for their description in practice. Potential applications of MDPs in the context of CRUTIAL could be the evaluation of recovery strategies or of fault/intrusion tolerance strategies

The solution of a MDP can be expressed as a strategy that selects among the actions available for each state, such that some function of the sequence of obtained rewards is maximized (or minimized). Formal languages can be defined to express the (quantitative) property that we want to be ensured by the strategies of an MDP. For example, probabilistic temporal logics can be used to specify properties such as “all strategies of the system reach a certain goal state with probability 0.99 or greater”, or “for all strategies, the average accumulated reward before the system crashes is less than 10”. Such probabilistic temporal logic properties can be considered in probabilistic model-checking analyses of MDP models, which rely on classical, efficient solution methods for MDPs.

3.1.5.3 Non-Exponential models

By non-exponential models, we identify all the stochastic models whose behaviour in time cannot be mapped into a Continuous Time homogeneous Markov Chain (CTMC). A common way to specify a non-exponential model is via a Non-Markovian Stochastic PN (or simply SPN). In recent years, several classes of SPN models have been developed which incorporate some non-exponential characteristics in their definition [Ajmone Marsan *et al.* 1989]. With the aim of specifying non-Markovian SPN models that are analytically tractable, three main lines of research can be envisaged [Ciardo *et al.* 1994, Bobbio *et al.* 1998]:

- an approach based on Markov regenerative theory
- an approach based on the use of supplementary variables
- an approach based on state space expansion.

The first line originated from a particular case of non-Markovian SPN, defined in [Ajmone Marsan & Chiola 1987], where, in each marking, a single transition is allowed to have associated a deterministic firing time with (Deterministic and SPN - DSPN). It has been observed in [Choi *et al.* 1994] that the marking process underlying a DSPN is a Markov Regenerative Process (MRGP) for which equations for the transition probability matrix in transient and in steady-state can be derived. A semantic generalization of the previous formulation has been considered in [Bobbio *et al.* 2000].

The second line resorts to the use of supplementary variables. The steady-state solution has been proposed in [German & Lindemann 1994], while the possibility of applying the methodology to the transient analysis has been explored in [Heindl & German 1997]. A comparison of numerical methods for the transient analysis of MRGPs applying the Markov regenerative theory and the method of the supplementary variables has been presented in [German *et al.* 1995b].

The third line of research, aimed at affording the solution of non-Markovian SPN, is based on the expansion of the reachability graph of the basic PN. In this approach, the original non-Markovian marking process is approximated by means of a CTMC defined over an augmented state space. The expansion technique can be realized by assigning to each PN-transition a continuous Phase-type (PH) distributed random variable. The merit of this approach is the intrinsic flexibility and the possibility of a computer implementation starting from the basic specification at the PN level, so that all the solution steps can be hidden from the modeler [Cumani 1985]. The drawback of this approach is, of course, the explosion of the state space that can be alleviated by resorting to the use of Kronecker operators for matrices. A more recent and interesting modification of the expansion technique, resorts to the use of discrete PH-type random variables [Ciardo 1995], so that the continuous-time marking process is approximated by an expanded discrete-time Markov chain (DTMC) [Bobbio & Horváth 2001].

3.1.5.4 Hybrid Discrete-Continuous state space models

In models with discrete state space, the dynamic evolution of the system in time can be represented as a sequence of transitions among discrete states. Paradigmatic models in this category are CTMC or models obtained from all the different variations of Petri Nets and High-Level Petri Nets with discrete tokens. Hybrid models combine discrete as well as continuous variables in the same framework, so that the state space of the model is partly discrete and partly continuous. Two main modelling approaches have been recently proposed to deal with hybrid systems: Hybrid Automata and Fluid Petri Nets. Typical examples of hybrid systems are discrete controllers that control continuous variables.

Hybrid automata - A hybrid automaton [Alur *et al.* 1995, Alur *et al.* 1996] is a finite state machine whose nodes (called control modes) contain real valued variables with a definition of their first derivatives and possible bounds on their values. The edges represent discrete events and are labelled with guarded assignments on the real variables. Hence, an hybrid automata transition among discrete states is governed by the value of continuous variables. Given a hybrid automaton and a legal formula on its variables, the model checking problem [Henzinger *et al.* 1995] asks to compute a region that satisfies the predicate, or to find at least one counterexamples that contradicts the predicate. As with TA, properties concerning reachability of certain states, or those expressed using temporal logic, are typically of interest in the context of hybrid automata. For certain classes of hybrid automata, analysis can take

the form of exhaustive exploration throughout the state space of the model (or on an abstraction of the hybrid automaton): for models with complex continuous dynamics, such exhaustive verification becomes prohibitive, and therefore methods such as simulation techniques can be employed.

Fluid Petri Net - Fluid Petri Nets (FPN) were introduced both in non-stochastic [Alla & David 1998] and stochastic [Trivedi & Kulkarni 1993] settings. The basic stochastic formalism was presented in [Trivedi & Kulkarni 1993] and refined in [Horton *et al.* 1998] and [Gribaudo *et al.* 2001]. Fluid stochastic Petri nets (FSPN) are stochastic Petri net based models with hybrid state space, in which some places may hold a discrete number of tokens, and some places a continuous quantity represented by a non-negative real number. Places that hold continuous quantities are referred to as fluid or continuous places, and the non-negative real number is said to represent the fluid level in the place.

Discrete tokens move along discrete arcs with the enabling and firing rules of standard SPN, while the fluid moves along special continuous (or fluid) arcs according to an assigned instantaneous flow rate. Fluid levels are changed either by fluid transitions according to fluid rate that can depend on the marking of the net or they can be set directly by a set arc to a given value when a transition fires. Inhibitor arcs (test arcs) disable (enable) a transition when a given number of token or a given quantity of fluid is present in a place. Hence, in the single formalism FPN, both discrete and continuous variables can be accommodated and their mutual interaction represented.

The stochastic process underlying an FSPN can be described by the approach of supplementary variables [Cox 1955]. In particular it is necessary to associate a supplementary variable to every fluid place of the FSPN [Gribaudo *et al.* 2001]. Having introduced the supplementary variables, the stochastic behaviour can be described by a set of differential equations. In general the solution of the set of differential equations describing an FSPN is not trivial. In very simple cases (single fluid place and simple dependence structure) closed form solutions can be found by spectral decomposition. In more complex cases discretization techniques can be applied, see [Horton *et al.* 1998, Gribaudo & Horváth 2002, Horváth & Gribaudo 2002]. In case of more than two fluid places the analytical solution of the set of differential equations is not feasible and simulation can be applied to get the solution [Gribaudo & Sereno 2000].

The fact that in a FSPN the firing rate can depend on the actual fluid level of the fluid places gives the possibility of implementing non-exponential delays. In particular, it is possible to model deterministic delays which can be used to model deadlines. Delays with finite support distributions can be implemented as well. Moreover, the continuous quantity may model time as well which allows the stochastic marking process associated to the model to have a complex time-dependent behaviour giving the opportunity of representing non-Markovian processes by means of FSPN [Gribaudo et al. 1999].

A comparison of the modelling power of Hybrid automata and FPN is given in [Tuffin *et al.* 2001, Gribaudo *et al.* 2003].

3.1.6 Modelling and evaluation wrt to malicious threats

As discussed in Section 2, malicious faults represent a serious threat to the dependability and resilience of the power grid and the corresponding information infrastructure. It is necessary to have appropriate methodologies and tools to support the analysis and evaluation of their impacts. Four main classes of evaluation methods can be distinguished to support these analyses: 1) Security evaluation criteria, 2) Risk assessment, 3) Model-based quantitative evaluation, and 4) experimental evaluation.

In the sequel, we present each of these methods and briefly summarize the corresponding state of the art.

3.1.6.1 Security evaluation criteria

The most common approach generally used for evaluating security is based on the assumption that a proper design and development process would be sufficient to prevent from malicious threats. Accordingly, several security evaluation criteria have been developed to assess the security of computer based systems and compare their ability to cope with malicious faults.

The first evaluation criteria are the famous "*Trusted Computer Security Evaluation Criteria"*, also known as TCSEC or "*orange book"* [TCSEC 1985] published by the Department of Defense in the USA. These criteria, based both on lists of security functions to be fulfilled and on the techniques used to verify them, lead to seven evaluation levels (in ascending order of security: D, C1, C2, B1, B2, B3, A1). The main goal of these criteria was primarily to meet DoD's requirements, i.e., priority has been initially given to confidentiality rather than integrity. Later, new criteria (the *federal criteria*) have been defined by the NIST (*National Institute of Standards and Technology*) and NSA (*National Security Agency*) [NIST-NSA 1992], to better take account of the various aspects of security, including confidentiality, integrity and availability. Evaluation based on these criteria is focused on "products" (isolated elements), rather than "systems" (products in their operating environment). Unlike the Orange Book, these criteria explicitly separate functional aspects from those related to development and from those related to *assurance* (or verification), each being assessed using multiple levels.

In fact, the idea of separating functionality requirements from assurance ones was already adopted in the European *standardized* criteria or ITSEC (*Information Technology Security Evaluation Criteria*) [ITSEC 1991] where ten functionality classes have been predefined, the first five taking up the functionalities of categories C1 to B3 defined in the Orange Book. Five other functionality classes were defined for high integrity systems, high availability systems, high integrity transmission systems, high confidentiality transmission systems and, finally, high integrity and confidentiality networks. However, other functionality combinations could be defined (if required) for a specific system or application. With regard to *assurance*, six levels are defined, denoted E1 to E6, from the least to the most demanding. *Efficiency assurance* criteria are also defined to evaluate the pertinence and cohesion of functionalities, the resistance of mechanisms, the vulnerability of the implementation as well as criteria linked to operation (ease of use, vulnerability in operation). Canada [CSEGC 1993] and Japan [JCSEC 1992] have also published their own evaluation criteria. The Common Criteria (CC) [CCIB 1998] represents the harmonization and the alignment of all these efforts. These standards have also been published as ISO Standards ISO/IEC 15408:2005 and ISO/IEC 18405:2005.

The CC structure provides great flexibility in the specification of secure products. Consumers and other parties can specify the security functionality of a product in terms of standard protection profiles, and independently select the evaluation assurance level from a defined set of seven increasing Evaluation Assurance Levels, from EAL1 up to EAL7. Depending on the chosen levels, different evaluation techniques have to be used by the evaluators. Further information on this topic are available in [CC 2006].

3.1.6.2 Risk assessment

The goal of risk assessment approaches is to analyse and determine the likelihood that identifiable threats will affect the target system security, weighing their occurrence with the

damage they might cause. Damage can be assessed by evaluating the average loss of money an attack might cause.

Risk assessment methodologies generally distinguish three main notions: threats, vulnerability and risks:

1) *Threats* correspond to the different possibilities that might exist for affecting some security objectives and the corresponding probabilities. Threats can be defined according to various dimensions: the source of the attack (internal or external to the system), the attacker's motivation, the attack process, the target and the result of the attack (consequences of the success of an attack), etc.
2) *Vulnerabilities* correspond to system weaknesses generally resulting from design faults, malicious or accidental, which enable the completion of a threat or the success of an attack.
3) *Risks* result from the combination of threats and vulnerabilities. Risks are evaluated either to obtain the best tradeoff between security and costs for a given system, or simply to compute the insurance premium to cover the risks.

Most systems have vulnerabilities. However, not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use.

Risk assessment approaches applied to security are mainly inspired from similar approaches commonly used in safety critical systems. Generally, the assessment takes into account the risks associated with accidental faults and natural disasters (fires, floods, earthquakes, software or erroneous data inputs, etc.) as well as malicious faults (terrorism, fraud, etc.).

Risk assessment can be qualitative only leading to the identification of threats and vulnerabilities and the different possibilities offered to the attackers to break into the target systems. Quantitative risk assessment can be carried out if probabilities and cost estimates can be associated to the threats taken into account in the analysis.

In the context of power systems and associated SCADA and ICT systems, several standards and working groups are emerging to develop risk assessment methodologies that are suited to this context A review of some of such initiatives is presented in [Dondossola *et al.* 2004, Schainker *et al.* 2006].

As an example, [Dondossola & Lamquet 2006] outline ongoing work carried by the CIGRE working group on "Security for Information Systems and Intranets in Electric Power Systems". They discuss the key aspects that a methodology for the security analysis of power utility information systems should cover. They also present a method called EPCSA that can be used to support: 1) the correlation of asset vulnerabilities, potential threats, and the possibility of attacks; 2) the definition of indexes to compute a qualitative estimate of the relevant properties of the system; and finally 3) the exploitation of correlations and indexes for scoring security failures and building the system security profile.

3.1.6.3 Model-based security evaluation

Security evaluation criteria and risk assessment methodologies are useful to support the analysis of security during the development process. However, they are widely recognized to be insufficient: a) to assess the impact of malicious attacks and vulnerabilities on the security of systems in operation, or b) to support architecture design tradeoffs based on quantitative criteria. Model-based evaluation approaches are commonly used in computer dependability to fulfil these objectives taking into account accidental faults. During the last decade, particular attention has been paid to exploring new approaches for security evaluation based on probabilistic models similar to those used in computer dependability. In the sequel we provide a short overview of related work addressing this topic. Additional information can be

found in [Nicol *et al.* 2004], in which the authors survey existing model-based techniques for evaluating system dependability, and summarize how they are now being extended to evaluate system security.

Early in the 90's, pioneering studies have been carried out within the framework of the ESPRIT PDCS project in an attempt to develop probabilistic methods for security evaluation analogous to those used for the evaluation of reliability. The objective was to define representative quantitative "measures" characterizing the capacity of a system to resist to attacks in operation. In [Littlewood *et al.* 1993], the authors introduce the concept of *effort* to derive measures such as the *mean effort to next failure* and others and present a stochastic approach to characterize security. An experimental study aiming at validating the feasibility of this approach was presented in [Brocklehurst *et al.* 1994, Jonsson & Olovsson 1997]. Controlled experiments where students had been asked to penetrate various systems (according to the so-called "*tiger team*" method) have been carried. In this approach, the system is considered as a "black box", since neither its components, nor the evolution of its configuration over time are represented.

Concurrently and in the context of the same European Project, LAAS-CNRS developed a modelling approach, based on a "white box" representation of the target system and its configuration, to model the influences of residual vulnerabilities in a system if misused by an attacker [Dacier et al. 1993]. The core of the method lies in a the definition of a formal model for describing the system vulnerabilities, called *privilege graph* [Dacier & Deswarte 1994]. The privilege graph highlights the various possibilities offered to an intruder to increase his privileges thanks to identified vulnerabilities or features of the system he has access to. This model is then used to derive attack scenarios characterizing how the attackers might navigate through the privilege graph and finally succeed in violating some security objectives. A Markov model is generated to derive probabilistic estimations of the ability of a system to resist attacks. These estimations are expressed as a *mean effort to security failure* (METF, similar to the MTTF measure for reliability), assessing the effort necessary for an attacker to realize a violation of a given security policy. The effort is considered as a multi-dimensional variable, taking into account the attacker competence and knowledge, the time needed to prepare and perform the attack, the efficiency of the protection mechanisms (e.g., the difficulty to guess a given password), etc. A software prototype tool has been developed to compute these measures, and has been used for a campaign of more than one year on a relatively complex system (a network of several hundred workstations in an academic environment). The results have been analyzed in [Ortalo *et al.* 1999], giving convincing arguments on the interest of the method, and the significance of the quantitative measures. These measures are not aimed to be interpreted in absolute terms or even used to compare the security of different systems: the objective is rather to allow administrators to monitor how the security of their system evolves as a function of configuration modifications (creation or suppression of users, installing new pieces of software, etc.) and identify the vulnerabilities that have the most impact on security.

Since the definition of the privilege graph, a variety of graph based approaches have been developed to support the description of vulnerabilities and attack scenarios (see e.g., [Phillips & Swiler 1998, Sheyner *et al.* 2002, Jajodia *et al.* 2003]), or to support alerts correlation in the context of intrusion detection [Cuppens & Miege 2002, Ning *et al.* 2002]. For example, the attack trees formalism proposed in [Schneier 1999] provides a methodical way, similar to fault trees, for representing how an attack can possibly be performed against a system. Basically, attacks are represented in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes. There are AND nodes and OR nodes for representing the various possibilities and alternatives for reaching the root node from the leaf nodes. An adaptation of this approach to take into account dependencies between vulnerabilities is proposed in [Balzarotti *et al.* 2006]. An example of application of attack trees to SCADA systems is presented in [Byres *et al.* 2004], in which the authors identified eleven attacker goals and associated security vulnerabilities in the specification and development of

typical SCADA systems. Their application was qualitative as the attack tree analysis was used only to identify attack scenarios and rank them according to severity of impact, probability of detection and level of difficulty.

Besides the studies mentioned above, other applications of graph based approaches and stochastic models to security can be found in [Nicol *et al.* 2004]. We can mention in particular the models proposed in [Madan *et al.* 2002, Gupta *et al.* 2003, Wang *et al.* 2003] targeting intrusion-tolerant systems. Generally, a state-based approach using Markov or semi-Markov models is used and quantitative measures are associated to particular states identifying failures at the system level with respect to high-level properties such as availability, integrity, or confidentiality. These models are processed using traditional Markov or Semi-Markov chain solution techniques.

For the sake of completeness, it is also worth to mention other types of stochastic models that have been explored in the literature in the context of security. These include e.g., epidemiology models or interactive Markov chains for studying malware propagations (see e.g., [Staniford *et al.* 2002, Zou *et al.* 2002, Garetto *et al.* 2003, Zou *et al.* 2005], models based on complex network theory to analyse the vulnerability of networked systems to cascading attacks [Crucitti *et al.* 2004b], game theory-based models for characterizing attackers behaviours and analyzing impact on security [Lye & Wing 2005, Sallhammar *et al.* 2005, Sallhammar *et al.* 2006].

3.1.6.4 Experimental evaluation

Model-based evaluation approaches rely on assumptions that need to be validated using real data collected during controlled experiments or from the field. In recent years, several initiatives and experimental studies have emerged for collecting and analyzing real data characterizing attacks and malicious activities on the internet. We can mention for example the Internet Motion Sensor project [Bailey *et al.* 2005], darknets [Cymru 2004], network telescopes [CAIDA], Dshield [DShield] and CADHo [Ealata *et al.* 2005].

The techniques used in the context of the Internet Motion Sensor, darknets and network telescopes are based on a similar approach: they use a fraction of unused IP space and passively monitor all incoming traffic, which most probably results from malicious activities. Dshield centralizes and analyses data collected from firewall logs or by intrusion detection systems from different sources all around the world. These projects provide valuable information for the identification and analysis of malicious activities on the Internet. Nevertheless, such information is not sufficient to model attack processes and analyze their impact on the security of the targeted machines.

The approach adopted by the CADHo project is aimed at addressing this objective, based on the deployment of a distributed platform of low-interaction honeypots that gathers data suitable to analyze the attack processes targeting a large number of machines connected to the Internet. A honeypot is a machine connected to a network but that no one is supposed to use. If a connection occurs, it must be, at best an accidental error or, more likely, an attempt to attack the machine. As of today, around 40 honeypot platforms have been deployed at various sites from academia and industry in almost 30 different countries over the five continents. The data gathered from the honeypot platforms include payload of all packets sent to or from these honeypots, and additional information to facilitate its analysis, such as the IP geographical localization of packets' source addresses, the OS of the attacking machine, the local time of the source, etc. Several analyses and interesting conclusions have been derived based on the collected data as detailed e.g., in the publications available at [Leurré.com]. Besides carrying out qualitative analyses and identifying trends, preliminary stochastic models have been elaborated to capture some characteristics of the attack processes observed on the honeypot platforms (see e.g., [Kaâniche *et al.* 2006]). The first results of these analyses offer positive insight regarding the possibility to use such data to

model attack processes happening over the Internet. Additional experiments based on high-interaction honeypots have been also carried out in [Alata *et al.* 2006] in order to learn about the attackers behaviours and activities once they had manage to gain access into a new target machine and try to progress into a network to obtain additional privileges. One of the objectives of these experiments is to validate the assumptions on attackers behaviours elaborated in the model-based evaluation approach discussed in [Ortalo *et al.* 1999] to quantify security.

The projects discussed above highlight the importance of experimental evaluation approaches to understand attackers behaviours and to elaborate realistic assumptions that can be used in model-based evaluation approaches aimed at evaluating quantitative measures characterizing the capacity of systems to resist to attacks. However, such kinds of combined analyses are still at a preliminary stage and need to be further explored, in particular in the context of interdependent power systems and information system infrastructures. Honeypot-based techniques are one of the popular solutions that are currently explored for collecting the data needed to support these analyses. In particular, it is worth to mention that there are currently some initiatives aimed at the development of honeypots that are well suited to address the vulnerabilities and threats targeting SCADA and process control systems. We can mention for example the Scada Honeynet project that aims to extend the concept of honeynet to SCADA networks [Pothamsetty & Franz 2005]. We can also mention the recent creation in the United-States of US-CERT, for collecting incidents and vulnerabilities affecting SCADA and control systems and coordinating defence against and response to cyber attacks (*http://www.us-cert.gov/control_systems*). On the other hand, the Department of Energy (DoE) in the United-States have launched a national SCADA Testbed (NSTB) to identify and remediate SCADA vulnerabilities and recommend security standards to protect the critical energy infrastructures. The outputs expected from these sources will be useful to support security analysis and evaluation methods in the context of interdependent power and information infrastructures.

3.1.6.5 Discussion

Model-based and experimental evaluation approaches for quantifying security are still at an exploratory stage. There are several challenging issues that must be addressed, including in particular the definition of widely accepted metrics that are representative of security properties and appropriate models that are able to evaluate such metrics. Also, so far the evaluation of dependability properties and security properties have been generally addressed separately. Clearly, there is a need for a comprehensive modelling framework that can be used to assess the impact of accidental faults as well as malicious threats in an integrated way. Generalization and extensions to the context of interdependent information and power distribution systems need also to be explored.

3.2 Interdependencies modelling in critical infrastructures

This Section provides firstly an overview of work related to the modelling of cascading failures and blackouts in the context of power system infrastructures. Then, it outlines some related cooperative research projects and initiatives dealing with the modelling and analysis of interdependent critical infrastructures.

3.2.1 Modelling of cascading failures and blackouts

In this section, we provide a summary of related work dealing with the modelling of the types of failures that are characteristic of interdependent infrastructures, in particular in the context of power systems infrastructures. We do not cover modelling studies addressing the reliability and availability evaluation of power systems. An extensive source of information on

this topic can found in the bibliography available in [Allan *et al.* 1999, Billinton *et al.* 2001, Bansal *et al.* 2002].

Among the three relevant types of failures in interdependent infrastructures introduced in section 2, the modelling of cascading failures has received increasing interest in the past years, in particular after the large blackouts of electric power transmission systems in 1996 and 2003. Several research papers and modelling studies have been published on this topic in particular by the Consortium for Electric Reliability Technology Solutions (CERTS) in the United-States [Dobson & Carreras 2005]. In the following we provide a short summary of recent work dealing with the modelling of cascading failures based in particular on the work carried out by CERTS.

Published studies on the analysis and modelling of cascading failures and power blackouts can be grouped into two categories:

- Statistical analysis and probability distribution fitting based on historical data collected from past blackouts.
- Development of analytical or simulation models aimed at describing cascading failures and studying blackout dynamics

In the following, we provide a short summary of work for each of these categories.

3.2.1.1 Statistical analysis of Blackout data

Using historical data collected on past blackouts several studies have been carried out to identify probability distributions that provide a good statistical fit to this data, considering e.g., the frequency and the size (amount of unserved energy) of the blackouts. The ultimate objective is to develop predictive models that can be used for planning purposes.

The North American Electric Reliability Council (NERC) has a documented list summarizing the disturbances and major blackouts of the North American power transmission system since 1984 [NERC, Adler *et al.* 1994]). Several statistical analyses of this or similar data exist in the literature. The main observation is that the probability distribution of the blackout data does not decrease exponentially with the size of the blackout, but rather has a heavy-tail distribution that is fairly close to a power law [Chen *et al.* 2001, Talukdar *et al.* 2003, Carreras *et al.* 2004b, Hines *et al.* 2006]. In [Carreras *et al.* 2004b], the authors argue that the power law and the properties of the transmission system indicate the existence of self-organized criticality [Bak *et al.* 1987] in the nature of power systems dynamics. [Weron & Simonsen 2006] question the appropriateness of applying self-organized criticality models to the NERC data set, but confirm the existence of a fatter-than exponential tail in the distribution. Moreover, the results presented in [Chen & McCalley 2004] suggest that Negative Binomial model provides a better fit to the blackout and transmission line outages data than the exponential or power law distributions. Other possible alternative distributions are discussed in [Chen *et al.* 2006].

3.2.1.2 Cascading failure models

A large literature has been dedicated recently to the elaboration of analytic or simulation based models that are able to capture the dynamics of cascading failures and blackouts. A brief review of related research addressing this topic is given hereafter. A more detailed state-of-the art can be found in [Dobson *et al.* 2004a, Anghel *et al.* 2007]. In particular, the stochastic model introduced in [Anghel *et al.* 2007], and inspired by [Dobson *et al.* 2001], attempts to provide a comprehensive representation of the complex behaviour of both the grid dynamics under random perturbations and the operators response to the contingency events.

The main objective of the approaches discussed in the sequel is to build analytical or simulation models that describe how a sequence of related events might lead to the occurrence of cascading failures and the associated probability.

In [Dobson *et al.* 2003, Dobson *et al.* 2005a], the authors present an idealized probabilistic model of cascading failures called CASCADE that is simple enough to be analytically tractable. It describes a general cascading process in which component failures weaken and further load the system so that components failures are more likely. The CASCADE model describes a finite number of identical components that fail when their load exceeds a threshold. As components fail, the system becomes more loaded, since a fixed amount of load is transferred to the other components, and cascading failures of further components become likely.

This cascade model and variants of it have been approximated in [Dobson *et al.* 2004b, Dobson *et al.* 2005b, Dobson *et al.* 2006] by a Galton-Watson branching process in which failures occur in stages, with each failure giving rise to a Poisson distribution of failures at the next stage. Some features of this cascade model are consistent with the simulations presented in [Carreras *et al.* 2004a].

The models mentioned above do not take into account the characteristics of power systems. Example of cascading failures models for a power transmission system have been proposed in [Carreras *et al.* 2002]. The OPA simulative model represents transmission lines, loads, generators and the operating limits on these components. Blackout cascades are essentially instantaneous events due to dynamical redistribution of power flows and are triggered by probabilistic failures of overloaded lines. The size of blackouts is determined by solving a standard LP optimization of the generation dispatch, consistent with the power flow equations and operational constraints, and the redistribution of power flows is calculated using a linear load flow approximation.

A simulation procedure is proposed in [Nedic 2003] to search for dangerous event developments (represented by an event tree) based on the concept of vulnerability region and on voltage stability. This procedure links different static and dynamic models used to assess transient stability, frequency response, voltage stability and steady state system conditions.

In [Rios *et al.* 2002] a simulation model is proposed to calculate the expected cost of outages, taking into account time-dependent phenomena (TDP) such a cascade tripping of elements due to overloads, malfunction of the protection system, potential power system instabilities and weather conditions.

Other examples emphasizing different aspects of the problem have been proposed e.g., in [Thorp *et al.* 1998, Bae & Thorp 1999, Chen & Thorp 2002, Chen *et al.* 2005], in which hidden failures of the protection system are represented. Their approach uses a probabilistic model to simulate the incorrect tripping of lines and generators due to hidden failures of line or generator protection systems. The distribution of power system blackout size is obtained using importance sampling and Monte-Carlo simulation.

Recently, new approaches using complex networks theory [Albert & Barabasi 2002a] have been also proposed for modelling cascading failures [Motter & Lai 2002, Watts 2002, Crucitti *et al.* 2004a, Chassin & Posse 2005, Kinney *et al.* 2005, Sun 2005]. These models are based on the analysis of the topology of the network characterizing the system and the evaluation of the resilience of the network to the removal of nodes and arcs, due either to random failures or to malicious attacks (see Section 3.1.5).

All the models discussed above adopt a simplified representation of the power system, assuming that the overloading of system components eventually leads to the collapse of the global system. However, these models do not take into account explicitly the complex interactions and interdependencies between the power infrastructure and the ICT

infrastructures. Moreover, the modelling of escalating failures is not addressed. Further work is needed in these directions.

3.2.2 Cooperative projects and initiatives

The vulnerability of critical infrastructures appears to be growing due to a number of factors, including growing demand, hectic transactions, growing number of stakeholders, high interconnection and interdependencies, complexity of control. Therefore, development of integrated interdisciplinary frameworks and related technologies for the provision of resilience, dependability and security in complex interconnected and heterogeneous communication networks and information infrastructures that underpin our economy and society is being promoted by research work programme, both at European and American levels.

Table 1 lists a few projects and initiatives, considered particularly relevant among those related to the CRUTIAL research agenda.

Title	Type	Start date-End date	Website
SAFEGUARD – Intelligent Agents Organisation to Enhance Dependability and Survivability of Large Complex Critical Infrastructure.	EU project - Funded under FP5	01/12/2001 31/05/2004	http://www.ist-safeguard.org/
IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems	EU IP Project – Funded under FP 6	01/02/2006 31/01/2009	http://www.irriis.org/
GRID: a coordination action on ICT vulnerabilities of power systems and the relevant defence methodologies	EU CA Project – Funded under FP 6	01/01/2006 31/12/2007	http://grid.jrc.it/
CI2RCO - Critical information infrastructure research coordination	EU CA Project – Funded under FP 6	01/03/2005 28/02/2007	http://www.ci2rco.org
RDS - Ricerca di Sistema	Italian Research Programme - Funded by the Italian Ministry of Industry, Trade and Crafts	Multiannual program active since 2000 until 2008	http://www.ricercadisistema.it/
TCIP: Trustworthy Cyber Infrastructure for the Power Grid	US project – Funded by NSF, Dep. of Energy and Dep. of Homeland Security	August 2005 August 2010	http://www.iti.uiuc.edu/tcip/

Table 1: Relevant projects and initiatives related to CRUTIAL research activity

SAFEGUARD was among the first European projects to focus on Large Complex Critical Infrastructures (LCCIs), such as distributed electricity and telecommunication networks. Its main goal was to enhance the dependability and survivability of LCCIs, through a systemic conceptual framework and an integrated software toolkit, employed within an intelligent multi-agent system. The scientific objective was to validate the applicability and efficacy of an intelligent agent organisation (and to develop related methodologies and methods) in support of LCCIs for ensuring their dependability and survivability. Technological objectives were the development of middleware for software agent components and their integration, applied to the project domain of interest.

The IRRIIS project aims at increasing the dependability and resilience of Large Complex Critical Infrastructures by introducing appropriate Middleware Improved Technology (MIT) based on Information and Communication Technology (ICT). The focus of the project is highly related to that of CRUTIAL, being on electricity and telecommunications and especially

on the interdependencies between these infrastructures, analyzed through the development of a synthetic simulation environment (SYNTEX).

The objective of GRID is to achieve consensus at the European level on the key issues involved by power systems vulnerabilities and the relevant defence methodologies, in view of the challenges driven by the transformation of the European power infrastructure. GRID wants to assess the needs of the EU power sector on these issues and achieve consensus among stakeholders and R&D institutions, so as to establish a roadmap for collaborative research in view of the forthcoming 7th framework programme. The focus is especially directed to: i) methods to assess reliability, security and risks affecting the power grid, and ii) management, control and protection schemes and the relevant architectures and devices.

The main objective of the CI2RCO project is to create and coordinate a European Taskforce to i) encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and ii) to establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security. CI2RCO will focus on activities across the EU-25 and ACC[2] that are essential to be carried out at European level and that require collaborative efforts involving the relevant players of research, research funding actors, policy-makers and CI-stakeholders. This is going to be accomplished by a set of coordination activities supporting the improvement of networking and coordination of national and European research policies, programmes and funding schemes.

The Italian Research Programme RdS has been set-up within the frame of the Public Interest Energy and performs research and development activities aimed at improving the economics, security and quality of the Italian electric system. The objective is to devise solutions to practical problems, taking into account dynamic evolutions and sustaining the changes dictated by international agreements (Kyoto), and evaluating the scientific-technological progresses. From 2000 to 2005 CESI (Centro Elettrotecnico Sperimentale Italiano) had been appointed to manage the funds assigned to the projects and its personnel (now moved in CESI RICERCA) were deeply involved in the development of the research activities. This Research Programme is structured in projects co-participated by the major research operators in the electrical field and academics, whose results are made public in form of reports or published papers (in Italian). More than 70 universities and research centres were involved in Italy and abroad. The Programme covers a wide-scope area of research in power generation, transmission and distribution grids, renewable and dispersed energy sources, also considering the physical hazards and environmental impact of these installations. Of specific interest for CRUTIAL are the activities in the area of power system regulation, control and automation including new control criteria for the power grids, probabilistic approaches to static and dynamic security assessment in the preventive control, ICT security analysis methodologies and robust ICT architectures that support the design and operation of networked automation applications, menaced by both accidental and malicious ICT faults. In particular, the hybrid model proposed in [Ciapessoni & Ferrarini 2005] to analyse hazards in the electrical power transmission system appears very interesting to CRUTIAL. This hybrid model combines: i) a Generalized Stochastic Petri Net to model the stochastic behaviour of the components of the electrical power transmission network (e.g., lines, busbars, transformers, switches and protections) and the propagation of the lightning among such components, and ii) a continuous part, based on the Kirchoff laws, in charge of the calculus of the electrical parameters (current and voltage), used to update the network topology. The dependability analysis of the electrical power transmission network has been carried out via simulation of the hybrid model. The software tool used for the construction of the hybrid model and for the simulation analysis is Modelica/Dymola (http://www.dynasim.com/index.htm).

[2] ACC means: Acceding and Candidate Countries

The TCIP NSF Cyber Trust Center was created in August 2005 to address the challenge of how to protect the US power grid. TCIP is working to provide the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements. The objective is to develop the necessary cyber building blocks and architecture, and the validation technology to quantify the amount of trust provided by the proposed approach. TCIP Focus Areas include: i) Reliable and Secure Computing Base; ii) Trustworthy Data Communications and Control; iii) Wide-area Trustworthy Information Exchange, and iv) Quantitative validation.

The CRUTIAL consortium will promote fruitful cooperation with the above listed projects/initiatives, and possibly with others that will be set up during the project's lifetime, mainly in terms of exchange of activity documents and participation to relevant events (such as thematic workshops organized by these projects). Some CRUTIAL partners are directly involved in a few of the mentioned initiatives: of course, they will act as a highly effective vehicle for cross-fertilization among related activities. Among the already established liaisons, the CRUTIAL consortium is part of the «IRRIIS Interest Group».

4 THE CRUTIAL PRELIMINARY MODELLING APPROACH

This Section provides preliminary directions about the approach followed in CRUTIAL for interdependencies modelling. Subsection 4.1 presents preliminary qualitative models for describing the typical failures that are characteristic of interdependent infrastructures, i.e., cascading, escalating and common-cause failures. The infrastructure interdependencies are modelled globally without explicitly describing their component behaviours. The detailed modelling of the infrastructures taking into account their internal structure is discussed in subsection 4.2 where a preliminary hierarchical modelling framework is presented based on the architectural descriptions and scenarios presented in [Brasca *et al.* 2006, CESI RICERCA 2006b, Leuven 2006]. The models discussed in Section 4.1. and Section 4.2 provide two complementary views for addressing the interdependencies modelling problem at two different abstraction levels.

4.1 Qualitative modelling of interdependencies

The aim of this section is to provide preliminary qualitative models of two interdependent infrastructures: the information infrastructure and the electricity infrastructure. As stated earlier, the interdependencies of these two infrastructures are increasing due to a growing connection of the power grid networks to the global information infrastructure, as a consequence of market deregulation and opening. These interdependencies increase the risk of failures or disruptions.

We focus on cascading, escalating outages and common-cause outages, which correspond the main causes of failures due to interdependencies as discussed in Section 2. Definitions for such events, when adopting outage and recuperation as generic terms, are reminded below:

- a *cascading outage* occurs when an outage in one infrastructure causes an outage of one or more component(s) in a second infrastructure;
- an *escalating outage* occurs when an existing outage in one infrastructure exacerbates an independent outage in another infrastructure, increasing its severity or the time for recuperation from this outage;
- a *common-cause outage* occurs when two or more infrastructures exhibit the outage in concomitance, due to some common cause, either internal or external.

It is noteworthy that these classes of outages are not independent: e.g., common-cause outages can cause cascading outages [Krings & Oman 2003].

We model the infrastructures globally, not explicitly modelling their components. The models presented are qualitative ones. They are built based on assumption related to the behaviour of the infrastructures as resulting from their mutual interdependencies. Indeed, the models describe scenarios that are likely to take place when outages occur.

In the remainder of this section, we will address outages in the electricity infrastructure and accidental outages in the information infrastructure and, considering the three classes of interdependencies, then we will illustrate briefly how malicious attacks can be addressed.

For the sake of clarity, and in order to avoid any confusion between the two infrastructures, we use specialized terms for the two infrastructures states and events as indicated by Table 1. These specialized terms apply when considering both sources of failures (accidental failures and malicious attacks). The first four lines correspond to states and events of each infrastructure as resulting from its own outages and recuperation actions, while the last line corresponds to the state of an infrastructure as resulting from the constraints imposed by the other infrastructure (i.e., a disruption in the electricity infrastructure leads the information infrastructure to a lessened state and a failure of the information infrastructure leads the electricity infrastructure to a weakened state. More details on these states will be given in the next section.

Table 1: States and events of the infrastructures

Generic	Information Infrastructure	Electricity Infrastructure
Normal operation	Working	Up
Outage	Failure, attack	Disruption
Dysfunction	Partially Failed	Partially Down, Lost
Recuperation	Recovery	Restoration
Constrained	Lessened	Weakened

4.1.1 Accidental outages

The aim is to model the infrastructures behaviour together taking into account the impact of accidental failures and disruptions, as well as their effects on both infrastructures. Modelling is carried out progressively:

- First, we model cascading events by analysing the constraints one infrastructure puts on the other one, assuming that the latter was in a normal operating state when an event occurs in the former.
- Then, we address cascading and escalating events considering successively:
  i) constraints of the information infrastructure on the electricity infrastructure,
  ii) constraints both ways (of the information infrastructure on the electricity infrastructure and of the electricity infrastructure on the information infrastructure).
- Finally, we address common-cause outages.

4.1.1.1 Modelling cascading outages

We analyse the impact of accidental failures on the information and electricity infrastructures assuming that the latter is in an Up state, then the impact of disruptions on electricity and information infrastructures assuming that the latter is in a Working state, before considering the combined impact of failures and disruptions in the next section.

Failures

Accidental failures, hardware- or software-induced, affecting the information infrastructure can be:

- masked failures, leading to latent errors,
- signalled failures.

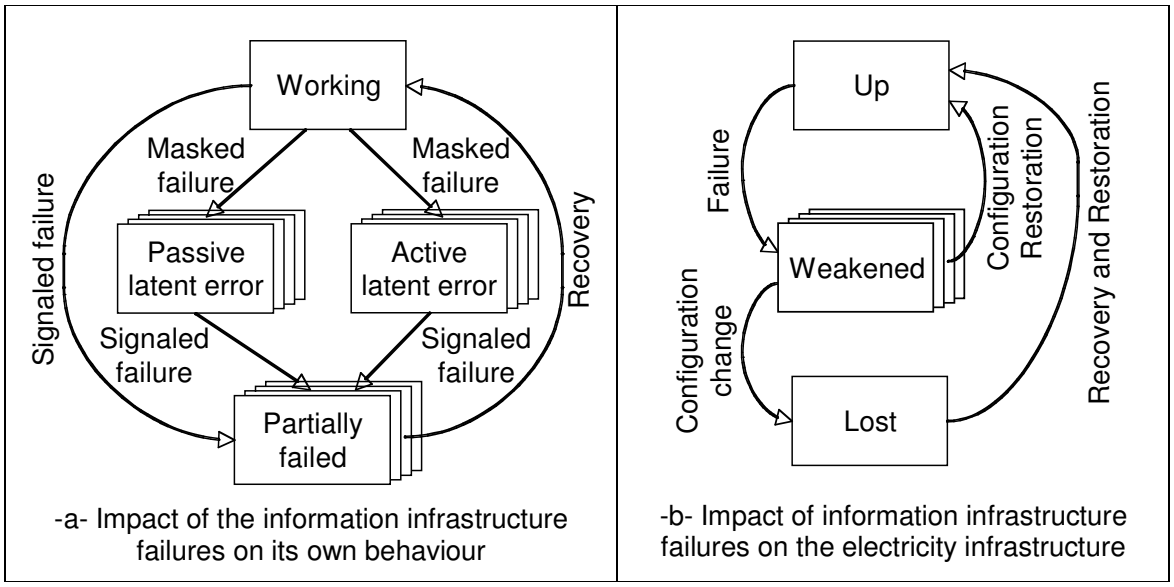
Latent errors can be:

- passive (i.e., without any action on the electricity infrastructure), but keeping the operators uninformed of possible disruptions occurring in the electricity infrastructure,
- active, provoking configuration changes in the electricity infrastructure.

After signalled failures, the information infrastructure is in partially failed states: the variety of functions and components of the information infrastructure, and its essential character of large network make unlikely total failure. Latent errors can accumulate, and signalled failures may take place when the information infrastructure is in latent error states. When the information infrastructure is in the partially failed state, recovery is necessary to bring it back to the working state.

Figure 4-a gives the state machine model of the information infrastructure taking into account its own failures. States presented by several boxes correspond in reality to a group of different states that are considered as equivalent with respect to the classification given in Table 1. For example all states with only one busbar isolated can be considered as equivalent irrespective of which busbar is isolated.

We assume that a failure in the information infrastructure puts some constraints on the electricity infrastructure (i.e., cascading outage), leading to a weakened electricity infrastructure (e.g., with a lower performance, unduly isolations, and unnecessary off-line trips of production plants or of transmission lines). From a Weakened state a configuration restoration leads the electricity infrastructure into an Up state. For the electricity infrastructure, the constraints may cause untimely configuration changes, leading to a Lost state (i.e., a blackout state), from which a restoration is required to bring back the electricity infrastructure into the Up state. Figure 4-b shows the constraint that the information infrastructure puts on the electricity infrastructure when the latter is in an Up state.



-a- Impact of the information infrastructure failures on its own behaviour

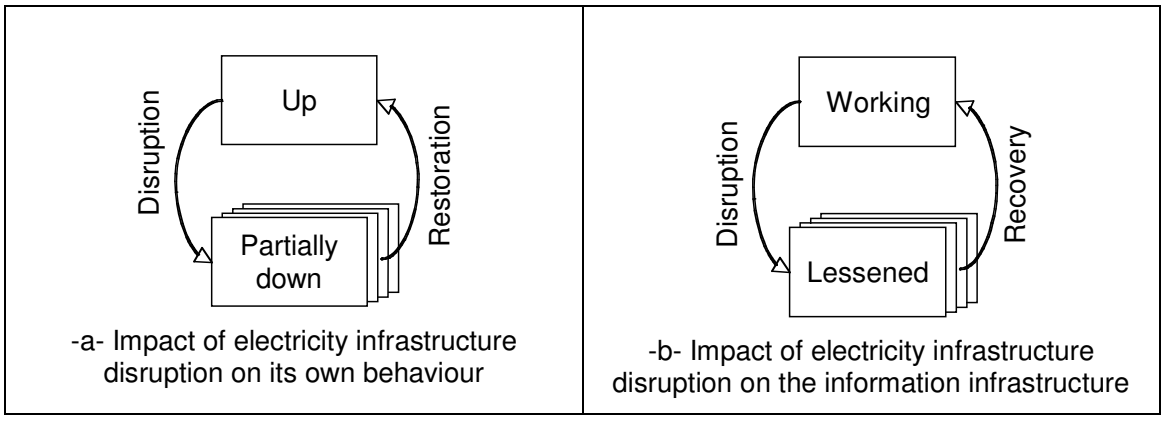
-b- Impact of information infrastructure failures on the electricity infrastructure

Figure 4: Impact of failures on infrastructures behaviour

Disruptions

We consider that disruptions lead the electricity infrastructure to be partially down, unless propagation within the infrastructure leads to loosing its control (e.g., a blackout of the power grid), because of an information infrastructure failure (this latter case corresponds to escalating events that will be covered in the next section). Figure 5-a gives the state machine model of the electricity infrastructure taking into account its own disruptions.

Also disruptions may lead the information infrastructure to a lessened state in which parts of the information infrastructure can no longer implement their functions, although they are not failed, due to constraints originating from disruptions of the electricity infrastructure. Figure 5-b shows the constraint that the electricity infrastructure puts on the information infrastructure assuming that the latter is in a working state.



-a- Impact of electricity infrastructure disruption on its own behaviour

-b- Impact of electricity infrastructure disruption on the information infrastructure

Figure 5: Impact of disruptions on infrastructures behaviour

Tables 2 and 3 summarise the states and events of each infrastructure, taking into account cascading events, as described above.

Table 2: States and events of the information infrastructure

Events	
Signalled failure	Detected failure
Masked failure	Undetected failure
Recovery	Action for bringing back the information infrastructure in its normal functioning after failure(s) occurred
States	
Working	The information infrastructure ensures normal control of the electricity infrastructure
Passive latent error	Parts of the information infrastructure are failed, which prevents monitoring of the electricity infrastructure: disruptions may remain unnoticed
Active latent error	Parts of the information infrastructure are failed, that may lead to unnecessary, and unnoticed configuration changes
Partially Failed	Parts of the information infrastructure are knowingly failed. Partially failed conditions are considered**:** the variety of functions and of the components of the infrastructure, and its essential character of large network make unlikely total failure
Lessened	Parts of the information infrastructure can no longer implement their functions, although they are not failed, due to constraints originating from disruptions of the electricity infrastructure, e.g., shortage of electricity supply of unprotected parts

Table 3: States and events of the electricity infrastructure

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

4.1.1.2 Modelling cascading and escalating outages

The global state machine model of the two infrastructures is built progressively:

- considering, in a first step, only the constraints of the information infrastructure on the electricity infrastructure,
- considering constraints of each infrastructure on the other.

Figure 6 gives a state machine model of the infrastructures, taking into account, only the constraints of the information infrastructure on the electricity infrastructure. The states are described in terms of the statuses of both infrastructures. Both cascading outages (states 3, 4) and escalating ones are evidenced, with a distinction of consequences of the latter in terms of time to restoration (state 6) and of severity (state 7). Dependency of the electricity infrastructure upon the information infrastructure is illustrated by the need for both recovery and restoration from states 6 and 7. This figure does not consider accumulation of disruptions in the electricity infrastructure

A noteworthy example of transitions from states 1 to 2, and from 2 to 7 relates to the August 2003 blackout in the USA and Canada: the failure of the monitoring software was one of the immediate causes of the blackout, as it prevented confining the electrical line incident, before its propagation across the power grid [US-Canada 2004].

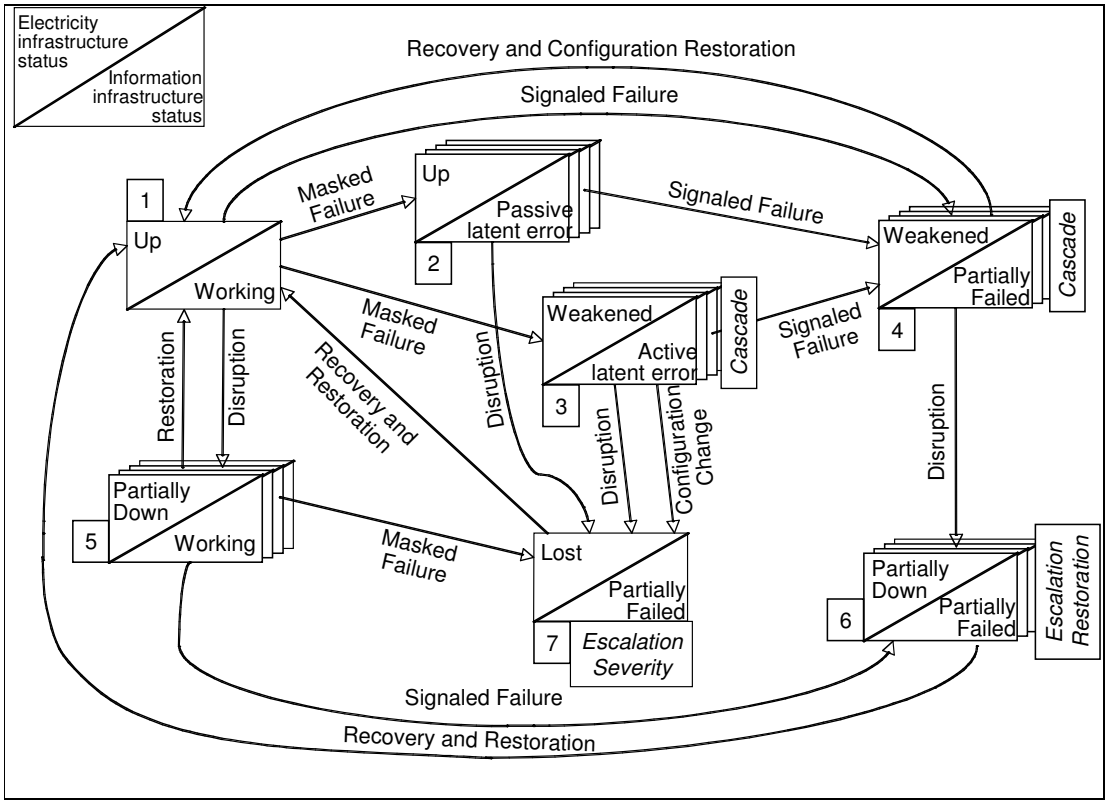


Figure 6: State Machine taking into account constraints of the information infrastructure on the electricity infrastructure

A Petri net representation of the model of Figure 3 is given by Figure 7, where the cascading and escalating mechanisms are evidenced. Such mechanisms are, in Petri net terms, synchronizations between the individual events of the infrastructures. Table 4 gives the correspondence between the states and events of Figures 6 and 7.

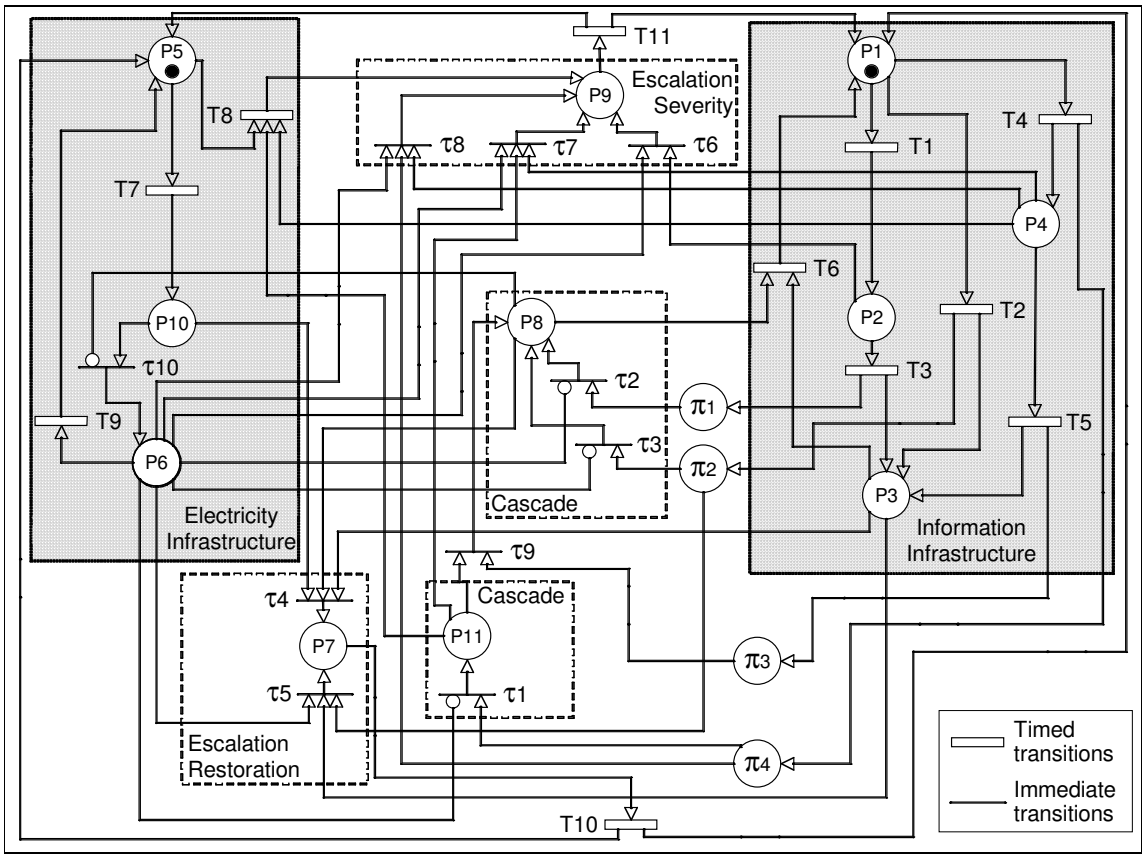


Figure 7: Example of a high level Petri net associated to the state machine of Figure 3

Table 4: Correspondence between states and events of the Petri net and Figure 3 model

States	Markings
1	P1, P5
2	P2,P5
3	P4,P5,P11
4	P3,P5,P8
5	P1,P6
6	P7
7	P9

State Machine Transitions	Petri Net Transitions
1 ↔ 2	T1
1 ↔ 3	T4 - τ1
1 ¼ 4	T2 - τ3
1 ¼ 5	T7 - τ10
2 ¼ 4	T3 - τ2
2 ¼ 7	T7 - τ10 - τ6
3 ¼ 4	T5 - τ9
3 ¼ 7 - config ch	T8
3 ¼ 7 - disruption	T7 - τ10 - τ7
4 ¼ 1	T6
4 ¼ 6	T7 - τ4
5 ¼ 1	T9
5 ¼ 6	T2 - τ5
5 ¼ 7	T1 - τ6 or T4 - τ8
6 ¼ 1	T10
7 ¼ 1	T11

This Petri net is very simple. In particular, it does not distinguish the individual states within a group of states represented by several boxes in Figure 6. For example, state 2 of Figure 6

that represents in reality a set of states is represented by a single state in the Petri net of Figure 7. The Petri net is given to illustrate how cascading and escalating events can be modelled in practice.

Figure 8 gives a state machine model of the infrastructures, taking into account the constraints of the electricity infrastructure on the information infrastructure in addition to those of the information infrastructure on the electricity infrastructure already considered in Figure 6. In addition, Figure 8 assumes possible accumulation of disruptions from states 5 to 7 and from the escalation restoration state 6 to the escalation severity state 8.

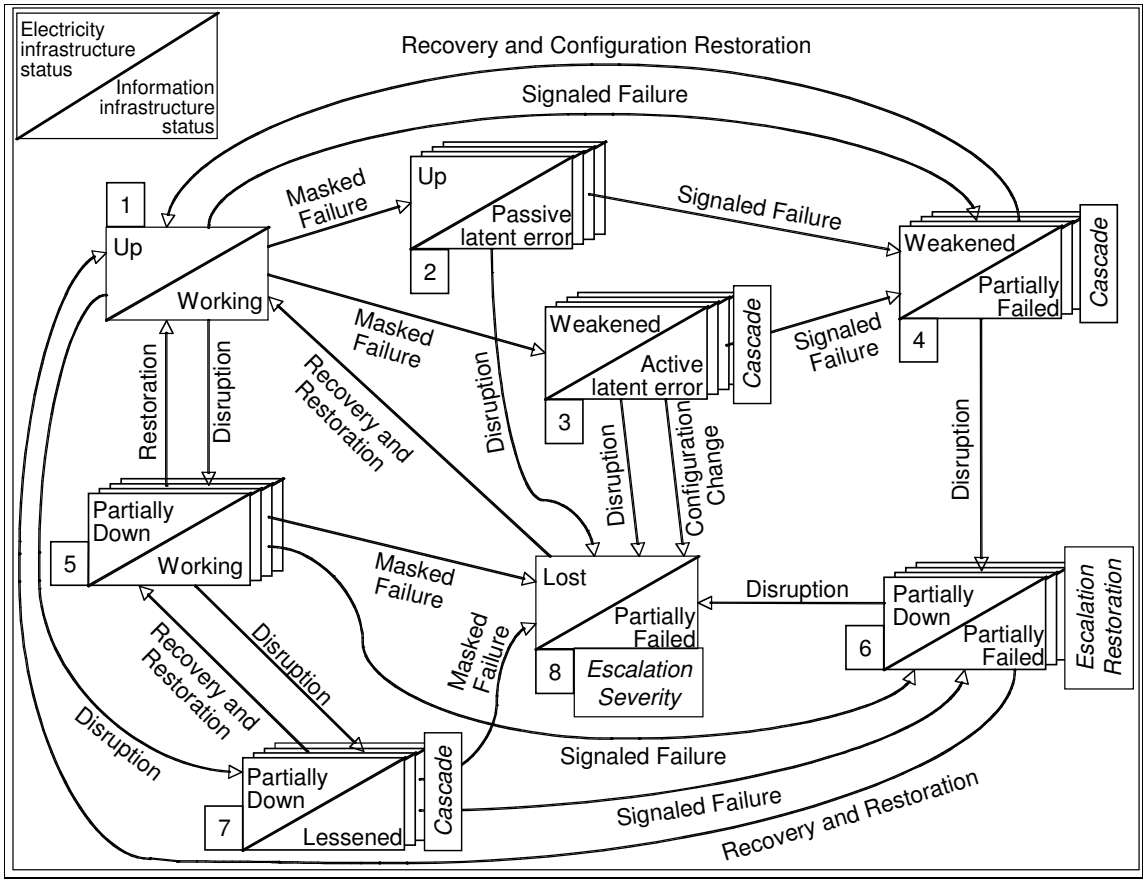


Figure 8: State machine model of the two infrastructures when considering accidental failures

4.1.1.3 Modelling common-cause outages

Figure 9 gives a model with respect to common-cause outages that would occur when the infrastructures are in normal operation, bringing the infrastructures into states 6 or 8 of Figure 8, i.e., to escalation. Should such outages occur in other states of the infrastructures of Figure 8 model, they would also lead to states 6 or 8.

Considering common-cause outages does not introduce additional states, they however add direct transitions from already existing states that do not exist when considering only cascading and escalating failures. The states of resulting model become almost totally interconnected.

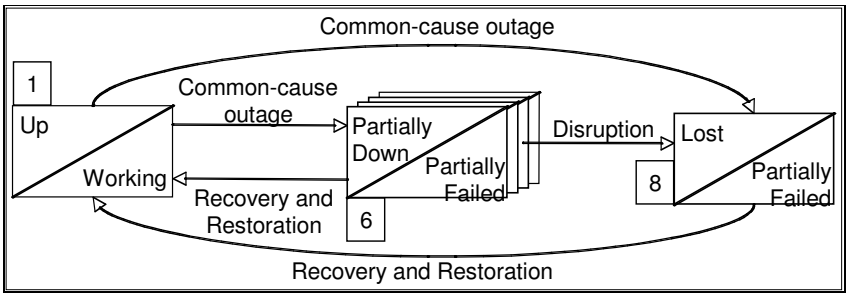


Figure 9: Common-cause outages

4.1.2 Malicious attacks

We consider malicious attacks of the information infrastructure and their consequences on the electricity infrastructure. A distinction has to be performed for both infrastructures between their real status and their apparent status. For the electricity infrastructure, the apparent status is as reported by the information infrastructure.

Attacks fall into two classes:

- *deceptive attacks* that are provoking unperceived malfunctions, thus similar to the latent errors previously considered,
- *perceptible attacks* creating detected damages.

Deceptive attacks can be:

- *passive* (i.e., without any direct action on the electricity infrastructure),
- *active*, provoking configuration changes in the electricity infrastructure.

Figure 10 gives the state machine model of the infrastructures. This model and the previous one are syntactically identical: they differ by the semantics of the states and of the inter-state transitions. Let us consider for example states 2 and 3.

In state 2, the effects of the passive deceptive attack are: i) the information infrastructure looks like working while it is in a partially failed state due to the attack, ii) it informs wrongly the operator that the electricity infrastructure is partially down, and as consequence iii) the operator performs some configuration changes in the electricity infrastructure leading it to a weakened state. Accumulation of configuration changes by the operator may lead the electricity infrastructure into a lost state.

In state 3, the effects of the active deceptive attack are: i) the information infrastructure looks like working while it is in a partially failed state due to the attack, ii) it performs some configuration changes in the electricity infrastructure leading it to a weakened state without informing the operator that the electricity infrastructure is partially down, for whom the electricity infrastructure appears if it were Up. Accumulation of configuration changes by the information infrastructure may lead the electricity infrastructure into a lost state.

The difference between states 2 and 3 is that in state 2 the operator has made some actions on the electricity infrastructure and is aware of the weakened state, while in state 3 the operator is not aware of the actions performed by the information infrastructure on the electricity infrastructure.

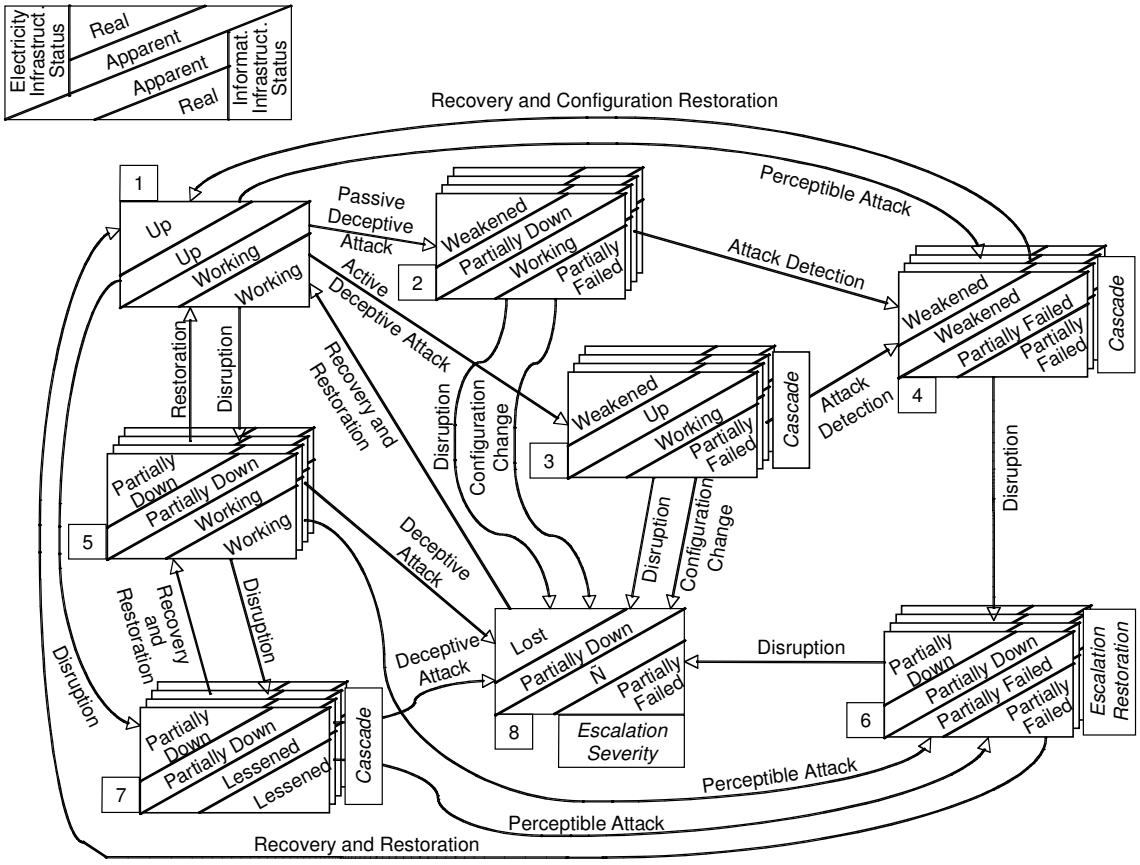


Figure 10: State machine model of the two infrastructures when considering malicious attacks

After detection of the attack, the apparent states of the infrastructures become identical to the real ones (state 4), in which Recovery and Configuration Restoration are necessary to bring back the infrastructures to their Working and Up states.

States 5, 6 and 7 are very similar respectively to states 5, 6 and 7 of Figure 8, except that in state 6 the information infrastructure is partially failed following a perceptive attack in Figure 10 and following a signalled failure in Figure 8.

In Figure 10, state 8 corresponds to a Lost state but the operator is not aware, he/she has been informed wrongly by the partially failed information infrastructure that it is partially down.

4.1.3 Conclusion

In this section we have introduced qualitative models allowing the analysis of the behaviour of the information and electricity infrastructures taking into account the effect of outages of each infrastructure on the other one. These models describe at a high level scenarios that may occur when outages occur and the relationship between the states of the two infrastructures.

4.2 Preliminary framework for the interdependencies modelling and quantitative evaluation

In this Section, an approach to a preliminary definition of the framework that could be used to characterize the interdependencies between the Electrical Infrastructure (EI) and its Information Technology based Control System (ITCS) is presented. Starting from the description of the EI and the ITCS, we have preliminarily characterized the state of the electrical infrastructure, the interdependencies between the two subsystems and identified the major modelling components, proposing a possible hierarchical composition approach.

Section 4.2.1 contains the main abbreviations used in the presentation of the framework. In Section 4.2.2 we identify the main system elements to be considered in the framework, basing on [CESI RICERCA 2006a] and [CESI RICERCA 2006b]. Then, the concept of state is defined in Section 4.2.3, both for the Electrical Infrastructure and for the Information Technology based Control System. In particular, a hybrid state is defined for the EI, composed by a discrete part and a continuous one. In Section 4.2.4 we identify possible failure models, both within the EI and ITCS individually, and considering their interdependencies. Next Section 4.2.5 briefly sketches the dynamic behaviour of the electrical power system. Section 4.2.6 proposes some representative measures of interest, while the modelling and evaluation framework is sketched in Section 4.2.7, in which we summarize the required functionalities and we give an example of its application.

4.2.1 Main abbreviations

- EPS: Electrical Power System
- EI: Electrical Infrastructure
- ITCS: Information Technology based Control System
- HG - LG: Huge Voltage - Medium and Low Voltage Generation plants
- TG - DG: Transmission - Distribution Grid
- HL – LL: Huge Voltage - Medium and Low Voltage Loads
- LTS: Local Telecontrol System
- RTS: Regional Telecontrol System
- NTS: National Telecontrol System
- LTC: Local Telecontrol Center
- ATC: Area Telecontrol Center

4.2.2 Logical scheme of the electrical power system

The content of this Section has been derived from [CESI RICERCA 2006a] and [CESI RICERCA 2006b]. The electrical power system (EPS) is logically structured in two interacting parts: Electrical Infrastructure (EI) and Information Technology based Control System (ITCS).

4.2.2.1 The Electrical Infrastructure

The EI represents the electrical infrastructure necessary to produce and to transport the electrical power towards the final users. It can be logically structured in different components, as shown in Figure 11: the transmission grid (TG), the distribution grid (DG), the huge voltage generation plants (HG), the medium and low voltage generation plants (LG), the huge voltage loads (HL), the medium and low voltage loads (LL).

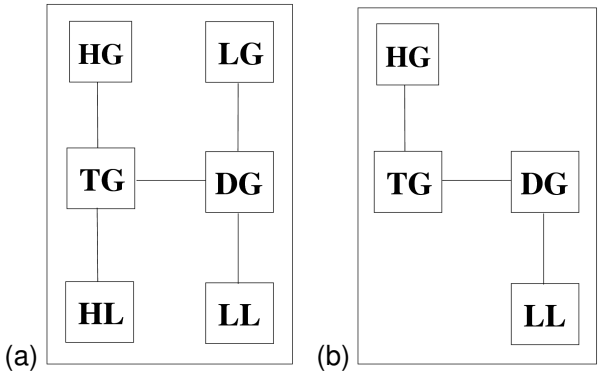


Figure 11: General (a) and typical (b) scheme of the EI

A typical scheme of EI is shown in Figure 11 where the components HL and LG are not present. Moreover, the distribution grid can be structured in two different medium and low voltage grids.

From a topological point of view, TG and DG can be considered like a network, or a graph, as shown in the example of Figure 12. The nodes of the graph represent the substations, while the arcs represent the power lines. The generators and the loads are nodes connected by arcs (power lines) to the nodes of the grid. Some nodes of the grid can be connected to nodes of the contiguous grid.

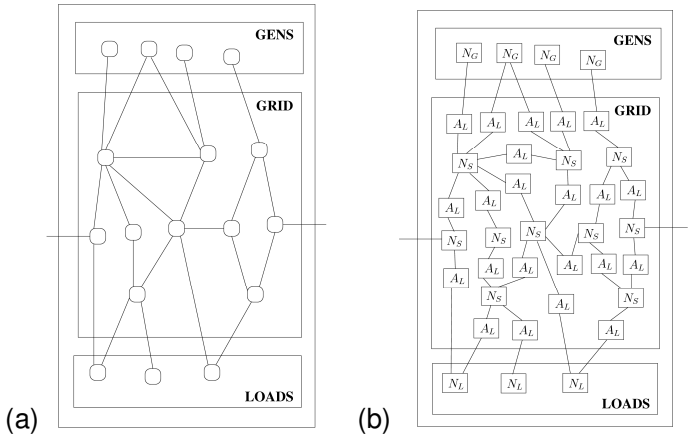


Figure 12: Example of meshed graph (a) and logical graph (b) for a dummy transmission grid

From the scheme of Figure 12 (a), the new logical scheme of Figure 12 (b) can be derived.

The logical schemes of the components N_G, N_L, N_S and A_L (not shown, for brevity) are obtained by grouping the main electrical equipments (transformer, bus-bar, breaker, switch, power line and protection) following an approach that has the advantage to simplify the logical representation.

The component N_S represents the parts common to all substations (e.g., the bus-bar). Breakers, switches, transformers and protection logics, which are physically part of a substation, are now included in the scheme for the new logical component A_L. In this way, only a few types of different A_L have to be considered. N_G and N_L represent a generation plant and a load, respectively.

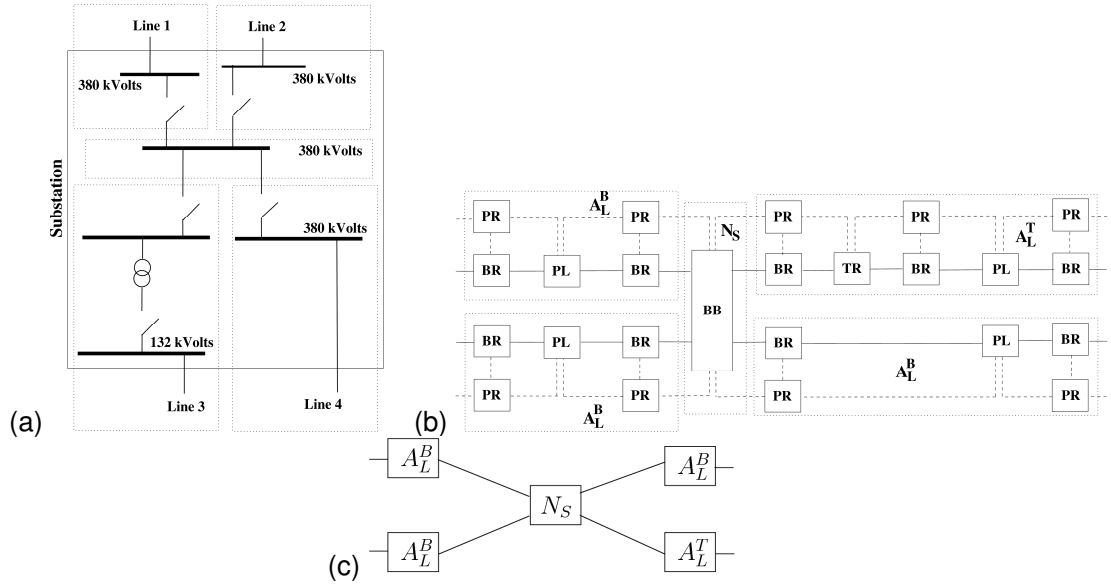


Figure 13: Example of scheme for a substation and the connected power lines: physical scheme (a), low level (b) and high level (c) logical schemes

In Figure 13 an example of physical and logical scheme for a substation and the connected power lines is shown, where two different types of component A_L are considered: $A^{B,L}$ and $A^{T,L}$.

4.2.2.2 The Information Technology Based Control System

ITCS implements the control system based on information technology. As shown in Figure 14, The main logical components of the *ITCS* are:

- the protection system (*PS*),
- the frequency regulation system (*FRS*),
- the voltage regulation system (*VRS*),
- the teleoperation (or telecontrol) system of the transmission grid (*TTOS*),
- the teleoperation (or telecontrol) system of the distribution grid (*DTOS*),

- the *TSO* transmission network (TSOcommNetw) and the *DSO* transmission network (DSOcommNetw).

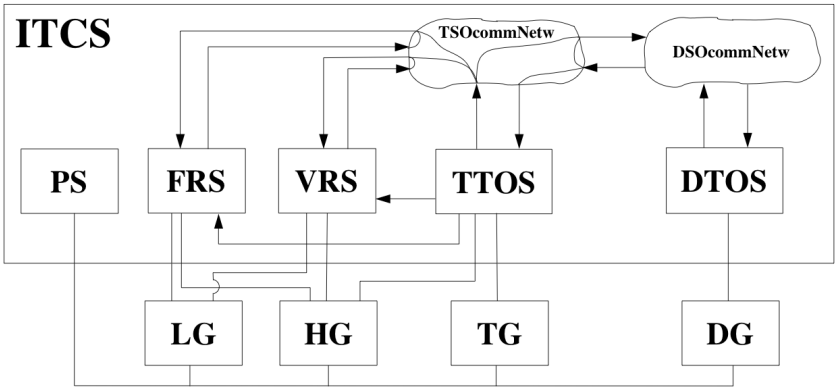


Figure 14: Logical scheme of the ITCS

The protection system is composed by a set of independent (or loosely connected) local protections. We can consider one local protection for each breaker of the EI. FRS has the goal to regulate the frequency of the single generators and along the transmission. It can receive information on the state of the grid from TTOS. VRS has the goal to guarantee that values of the voltages remain as constant as possible along the transmission grid in order to supply to the customers a voltage with good quality without interruptions.

At the current stage, the detailed logical structure of these components and that of the other subsystems involved in the ITCS system are not addressed, and the following discussion will only be limited to the TTOS and DTOS subsystems. In Figure 15 we depict a possible logical structure of TTOS and DTOS, where the components *LTS*, *RTS* and *NTS* of *TTOS*, and the components *LTC* and *ATC* of *DTOS* differ for their criticality and for the locality of their decisions.

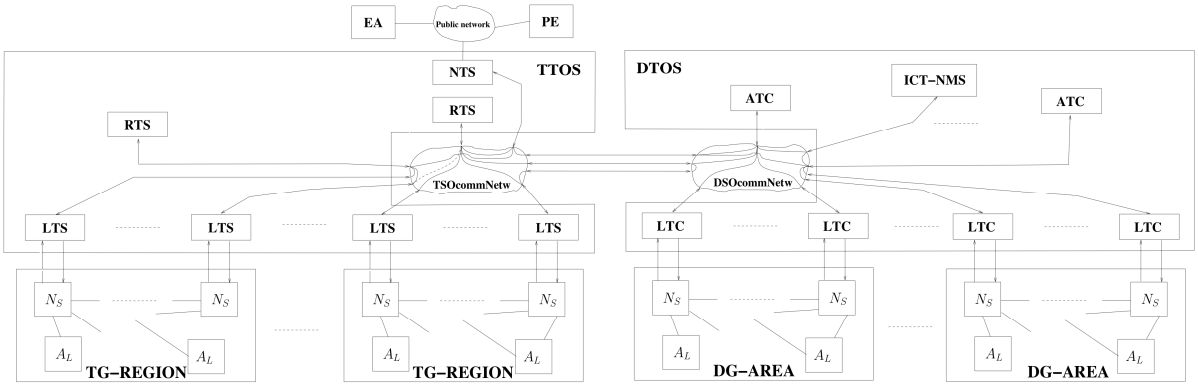


Figure 15: Logical scheme of TTOS and DTOS

The transmission and distribution grids are divided in homogeneous regions and areas, respectively. LTS and LTC guarantee the correct operation of substation equipment and reconfigures the substation in case of breakdown of some apparatus. They include the acquisition and control equipment (sensors and actuators). RTS and ATC monitors their region and area, respectively, in order to diagnose faults on the power lines. In case of

breakdowns, they choose the more suitable corrective actions to restore the functionality of the grid. Since the RTS and ATC were not directly connected to the substations, the corrective actions to adopt are communicated to the LTS or ATC of reference. NTS has the main function of supervising the entire grid and handling the planning of medium and long-term operations. NTS also assists the RTS (and ATC) to localize breakdowns on the power lines situated between two regions (two areas). LTS and LTC, such as RTS and ATC, cooperate to decide operation of load sheddings.

4.2.3 State definition for EI and ITCS

The state of the Electrical Infrastructure (EI) is an hybrid-state composed by a discrete part and a continuous one. It can be defined as a 7-tuple (T, V, F, I, A, P, Q), where:

- T represents the topology of the grid, i.e., the components N_S, N_G, N_L and A_L and their connections (as shown for example in Figure (b)). T could also include information on the direction of the current flow on each power line.

  This information is used to reconfigure the topology of the grid. Therefore, T can be described as an oriented graph where N_S, N_G and N_L are nodes and A_L are arcs.

- V, F, I, A, P and Q are the voltage, the frequency, the current flow, the angle, the active and reactive power associated to the components N_S, N_G, N_L and A_L (if applicable).

T represents the discrete part of the EI states, whereas V, F, I, A, P and Q represent the continuous part of the EI states [CESI RICERCA 2006a].

Following the state model as in [CESI RICERCA 2006a] (see Section 2.1.4), each state NORMAL, ALERT, EMERGENCY, IN EXTREMIS and RESTORATIVE of the EI can be described with different combinations of values of the 7-upla (T, V, F, I, A, P, Q).

For what concerns the ITCS state, we envision that such state to be discrete, in the sense that it is only composed by discrete values. Some possible states are “Working”, “Passive latent”, “Omission Failure”, etc. Its definition will be detailed during the project.

4.2.4 Failure model of EPS and Interdependencies

The failure model of the Electrical Power System (EPS) is presented in three steps. First, the failure model of the Electrical Infrastructure (EI) is sketched. Then, the failure model of the Information Technology based Control System is discussed. The third step consists of the ITCS-EI failure model, where the reciprocal impact of ITCS failures and of EI disruptions is analysed. Therefore, the model assumed for the disruptions of the EI and for the failures of the ITCS is based on their effects on the state of the EI.

Failure model of EI:

A disruption (or disturbance or contingency) is the unexpected failure or outage of a EI component, such as generator, power line, circuit breaker, bus-bar, or other electrical components. The main (electrical) disruptions, based on their effects on (single o multiple) components N_S, N_G, N_L and A_L, could be summarized in:

1) Transient or permanent disconnection of a component A_L, N_S, N_G, or N_L with the consequent separation of one or more components from the grid.
2) Transient or permanent failed disconnection of a component A_L, N_S, N_G, or N_L without isolation from the grid.

3) Transient or permanent overloads of A_L, N_S, N_G, or N_L.

4) Unexpected reduction of production of N_G.

5) Unexpected increase or reduction of demand of N_L.

6) Voltage collapse.

7) Underfrequency and loss of synchronism.

The disruptions listed at points from 3) to 7) represent changes of the electrical parameters of the components of the grid N_S, N_G, N_L and A_L.

The disruptions listed at points 1) and 7) represent changes of the topology of the grid T.

After the change of T, at least one or a combination of the values for V, F, I, A, P and Q will change. Whereas, when V, F, I, A, P and Q change, the topology T does not change.

Failure model of ITCS:

The failures of the ITCS components can be summarized in:

- (transient and permanent) omission failure,
- time failure,
- value failure and
- byzantine failure.

Here the focus is on the failures and not on their causes (internal HW/SW faults, malicious attacks, etc.).

ITCS-EI Failure model (interdependencies):

First, the impact of ITCS failures on EI is analysed. Failures in the ITCS impact on the state of the EI (i.e., on the topology T and on the values of V, F, I, A, P and Q), depending on the logical components affected by the failures, and obviously on the type of the failures.

For example, consequences of a failure of the component *LTS* associated to a component N_S, N_G, N_L and A_L can be:

- *Omission failure of LTS, fail silent LTS***.** No (reconfiguration) actions are performed on the components N_S or A_L.
- *Time failure of LTS.* The above (reconfiguration) actions on the components N_S or A_L are performed after a certain delay (or before the instant of time they are required).
- *Value failure of LTS.* Incorrect closing or opening of the power lines A_L directly connected to the component is performed. These events can occur both when the state of EI requires an action from ITCS (which is incorrect), and when the state of EI is normal and no action from ITCS is actually required.

Failures of the component *LTS* can also impact on the input values that the components *RTS* receive from *LTS*. These values can be omitted, delayed (or anticipated) or erroneous. Since reconfigurations required by *RTS* (or *NTS*) are actuated by the associated component *LTS*, a failure of a component *LTS* can also impact on the reconfigurations required by *RTS* (or *NTS*).

The failure of the component *RTS* (or *NTS*) corresponds to an erroneous (request of) reconfiguration of the state of the EI (including an unneeded reconfiguration) affecting one or more components of the controlled region. The effect of the failure of *RTS* (or *NTS*) on a

component N is the same as the failure of the component *LTS* associated to the component N. In the case of Byzantine failure these effects can be different for each component N.

In general, the failure of the components *LTS*, *RTS* and *NTS* may depend on the failures of the components connected to them through a (public or corporate) communication network.

Disruptions of EI on ITCS constitute a physical interdependency. Disruptions of the EI infrastructure impact on (parts of) the ITCS system by lessening its functionalities (till complete failure in the extreme case the disruption is a total blackout of the power grid). For example, a disruption may cause a partial blackout, that reduces the performance of the private or public network used by the ITCS. Then, the communication times degrade, leading to timing failures of the ITCS.

4.2.5 Dynamic behaviour of EPS

The hybrid-state of EI changes when the topology T of the system or the values for V, F, I, A, P and Q change, i.e., when one of the following events occurs:

- disruption (including failure of a local protection),
- activation of a protection local to the EI,
- voltage or frequency regulation or reconfiguration action by ITCS (including erroneous, delayed or not required action),
- maintenance actions on the EI.

Therefore, the state of EI can also change due to actions by the ITCS. These actions can be correctly activated by an event in the EI, or can be erroneously activated by a failure of the ITCS.

The discrete-state of ITCS can change when one of the following events occurs:

- failure of a component of the ITCS,
- disruption of the EI,
- recovery.

4.2.6 Measures of interest for the EPS

Dependability analysis of EPS based on a stochastic approach requires the definition of measures of performability, which is a unified measure proposed to simultaneously deal with performance and dependability. A set of measures specific for the EPS can be based on the following reward structure where costs and rewards are considered with respect to the point of the view of the power producers and distributors:

- To each generator a cost is associated, depending on: the generated power P, the type of generator, the economic loss implied by a breakdown of the generator.
- To each load a positive reward is associated, depending on: the consumed power, the criticality of the load.
- To each interruption of service supply a cost is associated, depending on: the difference between the required power and the available power for each load, the number of loads which will be powered off, the criticality of loads which will be powered off, duration of the interruption.

Generally, reconfigurations of EI impact on the performability measures, e.g., when loads are switched off/on or when consumed or generated power are modified.

4.2.7 Prominent Aspects of the EPS modelling framework

To model and evaluate the performability of EPS we first define a model representing the behaviour of the system at the needed level of detail, and then we solve it by simulation or analytically.

To represent and model the behaviour of EI and ITCS and their interactions, the following aspects should be considered.

Structural aspects:

- The system has a natural hierarchical structure, as shown in the examples of logical schemes of Section 4.2.2.
- At a certain level of detail, the system is composed by many similar components having the same logical structure, as shown, for example, in Figure 11(b) for the logical components N_S, N_G, N_L and A_L. In effect, these components can be grouped based on similar sub-components. All similar components can be considered non anonymous replicas having the same structure and different parameter values for the activities and the events represented.
- The topology of the grid and the electrical values associated to each component of the grid are part of the state of the EI.

Behavioural aspects:

- The time to disruptions of the components N_S, N_G, N_L and A_L depends also on the value of the electrical parameters associated to the components. A disruption of a component can propagate to contiguous components.
- The propagation time of a disruption should not be considered instantaneous.
- Protections can stop the propagation of a disruption by isolating from the grid the component affected by a disruption. The activation time of a protection should not be considered instantaneous. The correct activation of a protection depends also on the strength of the disruption and on the value of the electrical parameters associated to the protection component.
- The reaction time (with respect to the occurrence of a disruption), the failure time and erroneous activation time (when no disruptions have occurred) of a component (e.g., *LTS*, *RTS* and *NTS*) should be considered.
- The functions that implement the reconfiguration and regulation algorithms should be considered. These functions activate when EI is not in equilibrium; in such conditions, they receive as input the 7-tupla (T_i, V_i, F_i, C_i, A_i, P_i, Q_i) where the EI is not in equilibrium and produce as outputs the new 7-tupla (T_e, V_e, F_e, C_e, A_e, P_e, Q_e) which allows the equilibrium condition to be restored (that is, EI is back to the NORMAL state), if possible. If needed, the system's behaviour could be organized in phases, following the system state model shown in Figure 3.

To capture the above discussed structural and behavioural aspects, the modelling and evaluation framework should possess the following major characteristics, grouped into three categories: modelling power aspects (the basic modelling mechanisms required to build the EPS model), the modelling efficiency aspects (the advanced modelling mechanisms required to build the EPS model more efficiently), and the solution power aspects.

Modelling power:

- Different formalisms for different sub-models.
- Representation of continuous, discrete and hybrid state.
- Time distributions, probability distributions and conditions enabling the time consuming events which depend on the discrete or continuous state.
- The call to the function which implements the reconfiguration and regulation algorithms.
- Definition of performability measures.

Modelling efficiency:

- Hierarchical composition of the model.
- Possible organization in phases of the model (if needed).
- Composition of different sub-models.
- Replication of (anonymous and non anonymous) sub-models.
- Replicated and composed models can share part of state (common state).
- Duplication of a model (to make a copy of a model).
- Representation of discrete state.
- Compact representation for the topology of the grid (for T), for example, describing a part of the state of the system in terms of a matrix (incidence matrix [nodes x arcs]).
- Compact representation of continuous state (for V, F, I, A, P and Q), for example, describing a part of the state of the system in term of arrays, associating to each component of the EI grid (nodes and arcs) the values of V, F, I, A, P and Q (if any).

Solution power:

Analytical solution of the overall model (if possible). Problems could be: the explosion of the states of the model; an analytical solution method could not exist for the class of model considered, depending on the considered time distributions; the stiffness.

- Analytical solution of sub-models.
- Separate evaluation of different sub-models and combination of the results.
- Simulation (by existing automatic tools or ad hoc simulation software).

4.2.7.1 On the construction of the overall EPS model

In this Section we address the problem of building the overall model for the entire EPS, considering the logical scheme of the electrical grid as shown in Figure 12 (b).

The model construction should consist of the following steps:

1. Define the models M_N and M_A for each generic component N (representing a node of the grid, with N= N_S, N_G, N_L) and for A=A_L (representing an arc of the grid). To simplify the example we do not consider different schemes for each component.
2. Duplicate M_N and M_A for each specific component N and A, and set its individual parameters.

3. On the basis of the topology T, connect manually, the models M_N and M_A, by using a composition operator the models M_N and M_A, for each node N connected to an arc A.

When the number of components N and A is high, the construction of the model based on the above approach can be very expensive in terms of time and very error prone. The above process could be automated, defining a function which receives in input a incidence matrix describing the topology T of the grid and generates the composed model representing T.

Alternatively, a model describing a topology can be defined by using a compact approach based on replication and possibility to define part of the state of a system with an array (for the incidence matrix [nodes x arcs]). In this case, to construct a model representing a topology like that shown in Figure 12 (b), the following steps should be required, for *m* nodes N and *n* arcs A:

1. Define the model M_N and M_A for each generic component N (representing a node of the grid, with N= N_S, N_G, N_L) and for A=A_L.

2. Define a part of the state of M_N and M_A by using a matrix m x n T[i,j] of binary values (0,1), where $T[i,j]$=1 if the component i-th is connected to the component j-th, otherwise $T[i,j]$=0 (the values 1 and -1 can be used if it is needed to represent also the direction of the arc, i.e., if T is an oriented graph). The time distributions and the conditions in the model M_N can depend on the values of T. In particular, the i-th replica of M_N (or the j-th replica of M_A) can be defined as a function of $T[i,j]$, and can modify $T[i,j]$ (see below).

3. Define a hierarchical model by automatically replicating m times the model M_N, by assigning to each replica a different index, from 1 to m. The state defined with matrix T is common to all the replicated sub-models M_N. The parameters of the i-th replica can depend on the values of $T[i,j]$.

4. Define a hierarchical model by automatically replicating n times the model M_A, by assigning at each replica a different index, from 1 to n. The state defined with matrix T is common to all the replicated sub-models M_A. The replica j-th can depend by the values of the element $T[i,j]$.

Thus, it is possible to model a sub-system without constructing (or duplicating) manually the models for each single component N and A of the grid and without connecting each specific couple of models manually to obtain the required topology.

Following the same compact approach it is also possible to define the parameters of the replicas of the model M_N (or M_A) as a function of continuous state and to model fault propagation.

4.2.7.2 Discussion

We have discussed the major characteristics of the modelling and evaluation framework to properly assess the impact of interdependencies in EPS systems. Given the complexity of the system under analysis and of the steps required to implement the approach identified above, support by automatic tools is mandatory. The stochastic activity network (SAN) [Sanders & Meyer 2001] formalism and the framework of the tool Möbius [Daly *et al.* 2000] seem very suitable means to support the main characteristics described above. In fact, extended places having associated array of real numbers can be defined, thus allowing the definition of both discrete and continuous aspects of the system states. Moreover input gates, output gates, and parameters in the activities can be defined as a function of the extended places.

We are currently progressing in this work by investigating how to implement basic modelling characteristics of EPS in the Möbius environment. This would go in the direction of devising template models, to be combined together to represent the whole complex system under evaluation. Of course, detailed studies of the solution aspects need to be addressed too, to come out with a complete modelling and evaluation framework, suitable to quantitative assessment of interdependencies impact in electrical power systems.

5 CONCLUSION

This deliverable focused on the modelling and analysis of interdependencies between critical infrastructures, considering in particular two interdependent infrastructures studied in the context of CRUTIAL: the electric power infrastructure and the information infrastructures supporting management, control and maintenance functionality. Modelling activities are aimed at providing to the different actors involved in the development, operation, management and control of the infrastructures, and to the end users useful insights that will allow them: i) to understand how such interdependencies might impact the dependability and resilience of the delivered services, and ii) to assess the capabilities of the corresponding infrastructures and investigated architectural solutions to deal with the types of failures characteristic of such interdependencies, i.e., cascading, escalating and common cause failures, taking into account accidental faults as well as malicious threats.

This deliverable addressed three main goals. The first goal was to summarise the main challenges to be investigated for the analysis and modelling of interdependencies. The second goal was to review existing modelling approaches, techniques and tools that can be used to address these challenges, and to summarize related work and cooperative projects dealing with the modelling and evaluation of interdependent critical infrastructures in general, and power system infrastructures, in particular.

In the presentation of the state of knowledge, we have firstly presented the different types of models that are traditionally used to support dependability analysis and evaluation activities, emphasizing in particular the state-based modelling approaches that are well suited to address the challenges explored in the context of CRUTIAL. We have presented a detailed review of modelling approaches aimed at mastering the largeness of state-space models at the construction and the solution levels, and the available tools that can support the dependability evaluation activity. In addition, a particular attention has been focussed on the investigation of modelling techniques that can be used in the context of CRUTIAL to address other important challenging issues, such as the need to take into account timing constraints, to describe different types of uncertainties concerning the system dynamics and behaviour, or to model both discrete and continuous variables. Moreover, as malicious faults represent a serious threat to the dependability and resilience of critical infrastructures, a detailed discussion of existing modelling and evaluation approaches taking into account these faults is also presented. In the discussion of related work, we have also investigated the various works that have been carried out recently for modelling cascading failures, mainly in the context of power systems infrastructures. Such models are still at a preliminary stage and do not take into account the inherent characteristics of the infrastructures and the interdependencies between the power infrastructure and the corresponding information and control infrastructures. This is one of the objectives followed by CRUTIAL.

The third goal of this deliverable was to present preliminary directions about the approach followed in CRUTIAL for interdependencies modelling. Two main contributions have been obtained so far. Firstly, we have developed preliminary qualitative models for describing the typical failures that are characteristic of interdependent infrastructures, i.e., cascading, escalating and common-cause failures. The infrastructure interdependencies are modelled globally without explicitly describing their component behaviours. The second contribution concerns the development of a preliminary hierarchical model framework aimed at the

detailed modelling of the infrastructures taking into account their internal structure. The proposed model is based on the architectural descriptions and scenarios discussed in Workpackage 1.

The preliminary results obtained so far will be consolidated and extended in the future work. Besides progressing towards the implementation of the basic building blocks needed to describe the different subsystems of the infrastructures under study, and the definition of efficient means for the composition of the submodels corresponding to these building blocks, attention will be focused on the definition of a comprehensive modelling approach that will allow us to take into account both accidental and malicious faults in an integrated way. In addition detailed studies of the solution aspects need to be addressed too, to come out with a complete modelling and evaluation framework, suitable to quantitative assessment of interdependencies impact in electrical power systems.

REFERENCES

[Adler *et al.* 1994] R. Adler, S. Daniel, C. Heising, M. Lauby, R. Ludorf and T. White, "An IEEE Survey of US and Canadian Overhead Transmission outages at 230kV and above", *IEEE Transactions on Power Delivery*, 9 (1), pp.21-39, January 1994.

[Adve *et al.* 2000] V. S. Adve, R. Bagrodia, J. C. Browne, E. Deelman, A. Dube, E. Houstis, J. Rice, R. Sakellariou, D. Sundaram-Stukel, P. J. Teller and M. K. Vernon, "Poems: End-to-end performance design of large parallel adaptive computational systems", *IEEE Transactions on Software Engineering, Special Section of invited papers from the WOSP '98 Workshop*, 26 (11), pp.1027-1048, 2000.

[Ajmone Marsan *et al.* 1989] M. Ajmone Marsan, G. Balbo, A. Bobbio, G. Chiola, G. Conte and A. Cumani, "The Effect of Execution Policies on the Semantics and Analysis of Stochastic Petri Nets", *IEEE Transactions on Software Engineering*, 15 (7), pp.832-846, July 1989.

[Ajmone Marsan *et al.* 1995] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli and F. G., *Modelling with Generalized Stochastic Petri Nets,* John Wiley, 1995.

[Ajmone Marsan & Chiola 1987] M. Ajmone Marsan and G. Chiola, "On Petri nets with deterministic and exponentially distributed firing times", LNCS 266, pp.132-145, Springer-Verlag, 1987.

[Alata *et al.* 2006] E. Alata, V. Nicomette, M. Kaâniche, M. Dacier and M. Herrb, "Lessons Learned from the Deployment of a High-Interaction Honeypot", in *Sixth European Dependable Computing Conference (EDCC-6),* (Coimbra, Portugal), pp.39-44, IEEE Computer Society, 2006.

[Albert & Barabasi 2002a] Albert, R. and A.-L. Barabasi, "Statistical Mechanics of Complex Networks", *Review of Modern Physics*, 74, pp.47-97, 2002a.

[Albert & Barabasi 2002b] R. Albert and A.-L. Barabasi, "Statistical mechanics of complex networks", *Review Modern Physics*, 74 (47-97) 2002b.

[Alla & David 1998] H. Alla and R. David, "Continuous and Hybrid Petri Nets", *Journal of Systems Circuits and Computers*, 8 (1), pp.159-188, 1998.

[Allan *et al.* 1999] R. N. Allan, R. Billinton, A. M. Breipohl and C. H. Grigg, "Bibliography on the Application of Methods in Power System Reliability Evaluation 1992-1996", *IEEE Transactions on Power Systems*, 14 (1), pp.51-57, 1999.

[Alur *et al.* 1995] A. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis and S. Yovine, "The Algorithmic Analysis of Hybrid Systems", *Theoretical Computer Science* 138 (1), pp.3-34, 1995.

[Alur *et al.* 1996] A. Alur, T. A. Henzinger and P.-H. Ho, "Automatic symbolic verification of embedded systems", *IEEE Transaction Software Engineering*, 22 (181-201) 1996.

[Alur & Dill 1990] R. Alur and D. L. Dill, "Automata for modelling real-time systems", *17th International Colloquium on Automata, Languages and Programming (ICALP)*, 443, pp.322-335, 1990.

[Alur & Dill 1994] R. Alur and D. L. Dill, "A Theory of Timed Automata", *Theoretical Computer Science*, 126 (2), pp.183-235, 1994.

[Amin 2005] M. Amin, "Scanning the Technology—Energy Infrastructure Defense Systems", *Proceedings of the IEEE*, 93 (5), pp.861-75, 2005.

[Ammar & Rezaul Islam 1989] H. H. Ammar and S. M. Rezaul Islam, "Time scale decomposition of a class of generalized stochastic Petri net models", *IEEE Transactions on Software Engineering*, 15 (6), pp.809-820, 1989.

[Anghel *et al.* 2007] M. Anghel, K. A. Werly and A. E. Motter, "Stochastic Model for Power Grid Dynamics", in *40th Hawaii International Conference on System Sciences,* (Big Island, Hawaii), 2007.

[Avizienis *et al.* 2004] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions On Dependable And Secure Computing*, 1 (1), pp.11-33, January-March 2004.

[Bae & Thorp 1999] K. Bae and J. D. Thorp, "A Stochastic Study of Hidden Failures in Power System Protection", *Decision Support Systems*, 24, pp.259-268, 1999.

[Bailey *et al.* 2005] M. Bailey, E. Cooke, F. Jahanian and J. Nazario, "The Internet Motion Sensor - A Distributed Blackhole Monitoring System", in *Network and Distributed Systems Security Symposium (NDSS-2005),* (San Diego, CA, USA), 2005.

[Bak *et al.* 1987] P. Bak, C. Tang and K. Wiesenfeld, "Self-organized Criticality: an explanation of 1/f noise", *Physical Review Letters*, 59 (4), pp.381-384, 1987.

[Balakrishnan & Trivedi 1995] M. Balakrishnan and K. S. Trivedi, "Componentwise Decomposition for an Efficient Reliability Computation of Systems with Repairable Components", in *25th Int. Symposium on Fault-Tolerant Computing (FTCS-25),* (Pasadena, CA, USA), pp.259-268, IEEE Computer Society Press, 1995.

[Balan & Traldi 2003] A. O. Balan and L. Traldi, "Preprocessing minpaths for sum of disjoint products", *IEEE Transaction on Reliability*, 52 (3), pp.289-295, September 2003.

[Balbo 1995] G. Balbo, "On the success of stochastic Petri nets", in *6th International Workshop on Petri Nets and Performance Models (PNPM'95),* (Durham, NC, USA), pp.2-9, IEEE Computer Society, 1995.

[Balbo *et al.* 1986] G. Balbo, S. C. Bruell and S. Ghanta, "Combining Queuing Networks and Generalized Stochastic Petri Net Models for the Analysis of some Software Blocking Phenomena", *IEEE Transactions on Software Engineering*, SE-12, pp.561-576, 1986.

[Ballarini *et al.* 2000] S. Ballarini, S. Donatelli and G. Franceschinis, "Parametric Stochastic Well-Formed Nets and Compositional Modelling", in *21st International Conference on Application and Theory of Petri Nets,* (Aarhus, Denmark), Springer Verlag, 2000.

[Balsamo *et al.* 2004] S. Balsamo, A. Di Marci, P. Inverardi and S. Simeoni, "Model-based performance prediction in software development: A survey", *IEEE Transactions on Software Engineering*, 30 (5), pp.295-310, 2004.

[Balzarotti *et al.* 2006] D. Balzarotti, M. Monga and S. Sicari, "Assessing the Risk of Using Vulnerable Components", in *Quality of Protection: Security Measurements and Metrics* (D. Gollmann, M. Massacci and A. Yautsiukhin, Eds.), pp.65-78, Springer, 2006.

[Bansal *et al.* 2002] R. C. Bansal, T. S. Bhatti and D. P. Khotari, "Discussion of "Bibliography on the Application of Probability Methods in Power Methods in Power System Reliability Evaluation", *IEEE Transactions on Power Systems*, 17 (3), p.924, 2002.

[Baskett *et al.* 1975] F. Baskett, K. M. Chandy, R. R. Muntz and F. G. Palacios, "Open, closed, and mixed networks with different classes of customers", *Journal of the ACM*, 22 (2), pp.248-260, April 1975.

[Bause *et al.* 1998] F. Bause, P. Buchholz and P. Kemper, "A toolbox for functional and quantitative analysis of deds", in *Lecture Notes in Computer Science* (N. N. S. R. Puigjaner, and B. Serra, Ed.), LNCS 1469, pp.356-359, Springer-Verlag, 1998.

[Bechta-Dugan *et al.* 1992] J. Bechta-Dugan, S. J. Bavuso and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems", *IEEE Transactions on Reliability*, 41, pp.363-377, 1992.

[Bellman 1957] R. E. Bellman, *Dynamic Programming,* Princeton University Press, 1957.

[Béounes *et al.* 1993] C. Béounes, M. Aguéra, J. Arlat, C. Bourdeau, J.-E. Doucet, K. Kanoun, J.-C. Laprie, S. Metge, J. Moreira de Souza, D. Powell and P. Spiesser, "SURF-2: A Program for Dependability Evaluation of Complex Hardware and Software Systems", in *23rd IEEE Int. Symposium on Fault-Tolerant Computing (FTCS-23),* (Toulouse, France), pp.668-673, IEEE Computer Society Press, 1993.

[Bernardi 2003] S. Bernardi, *Building Stochastic Petri Net models for the Verification of Complex Software Systems,* PhD, Universita di Torino, 2003.

[Bernardi & Donatelli 2003] S. Bernardi and S. Donatelli, "Building Petri Net Scenarios for Dependable Automation Systems", in *10th International Workshop for Petri Nets and Performance Models (PNPM'2003),* (Urbana-Champaign, IL, USA), pp.72-81, IEEE Computer Society, 2003.

[Bernardi *et al.* 2001] S. Bernardi, S. Donatelli and A. Horváth, "Special section on the practical use of high-level Petri nets: Implementing compositionality for stochastic Petri nets. " *Journal of Software Tools for Technology Transfer (STTT).* pp.417-430, 2001.

[Bernardi *et al.* 2002] S. Bernardi, S. Donatelli and J. Merseguer, "From UML sequence diagrams and statecharts to analyzable Petri net models", in *3rd Workshop Software and Performance (WOSP'02),* pp.35-45, ACM Press, 2002.

[Bernardi & Merseguer 2006] S. Bernardi and J. Merseguer, "QoS Assessment via Stochastic Analysis", *IEEE Internet Computing* (May-June), pp.32-42, 2006.

[Bernardi & Merseguer 2007] S. Bernardi and J. Merseguer, "A UML Profile for Dependability Analysis of Real-Time Systems", in *Accepted for publication in the Workshop Software and Performance WOSP'07,* 2007.

[Berthomieu & Diaz 1991] B. Berthomieu and M. Diaz, "Modeling and Verification of Time Dependent Systems Using Time Petri Nets", *IEEE Transactions on Software Engineering*, 17 (3), pp.259-273, 1991.

[Berthomieu & Vernadat 2003] B. Berthomieu and F. Vernadat, "State class constructions for branching analysis of time Petri nets", in *9th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2003),* (Warsaw, Poland), pp.442-457, Springer-Verlag, 2003.

[Best *et al.* 1992] E. Best, R. Devillers and J. Hall, "The Petri box calculus: a new causal algebra with multilabel communication. In editor, Advances in Petri Nets, volume 609 of LNCS, pages 21-69. Springer Verlag, 1992." in *Advances in Petri Nets* (G. Rozenberg, Ed.), LNCS 609, pp.21-69, Springer-Verlag, 1992.

[Betous-Almeida & Kanoun 2004a] C. Betous-Almeida and K. Kanoun, "Construction and Stepwise Refinement of Dependability Models", *Performance Evaluation*, 56, pp.277-306, 2004a.

[Betous-Almeida & Kanoun 2004b] C. Betous-Almeida and K. Kanoun, "Dependability modelling of Intsrumentation and Control Systems: A Comparison of Competing Architectures", *Safety Science*, 42, pp.457-480, 2004b.

[Billinton *et al.* 2001] R. Billinton, M. Fotuhu-Firuzabad and L. Bertling, "Bibliography on the Application of Methods in Power System Reliability Evaluation 1996-1999", *IEEE Transactions on Power Systems*, 16 (4), pp.595-602, 2001.

[Bobbio & Codetta Raiteri 2004] A. Bobbio and D. Codetta Raiteri, "Parametric Fault-Trees with Dynamic Gates and Repair Boxes", in *Annual Reliablity and Maintainability Symposium (RAMS '04),* (Los-Angeles, CA, USA), pp.459-465, 2004.

[Bobbio *et al.* 2006] A. Bobbio, C. Ferraris and R. Terrugia, "New Challenges in Network Reliability Analysis", in *International Workshop on Complex Network and Infrastructure Protection (CNIP'2006),* (Rome, Italy), 2006.

[Bobbio *et al.* 2003] A. Bobbio, G. Franceschinis, R. Gaeta and L. Portinale, "Parametric Fault-Tree for the Dependability Analysis of Redundant Systems and its High Level Petri Net Semantics", *IEEE Transactions Software Engineering*, 29 (270-287) 2003.

[Bobbio & Horváth 2001] A. Bobbio and A. Horváth, "Petri nets with discrete phase timing: A bridge between stochastic and functional analysis", in *Second International Workshop on Models for Time-Critical Systems (MTCS 2001),* (Amsterdam, Nethetherlands), pp.22-38, 2001.

[Bobbio *et al.* 2001] A. Bobbio, L. Portinale, M. Minichino and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into bayesian networks", *Reliability Engineering and System Safety*, 71, pp.249-260, 2001.

[Bobbio *et al.* 2000] A. Bobbio, A. Puliafito and M. Telek, "A modeling framework to implement preemption policies in non-Markovian SPN", *IEEE Transactions Software Engineering*, 26, pp.36-54, 2000.

[Bobbio *et al.* 1998] A. Bobbio, A. Puliafito, M. Telek and K. Trivedi, "Recent developments in non-Markovian stochastic Petri nets", *Journal of Systems Circuits and Computers*, 8 (1), pp.119-158, 1998.

[Bobbio & Trivedi 1986] A. Bobbio and K. Trivedi, "An Aggregation Technique for the Transient Analysis of Stiff Markov Chains", *IEEE Transactions on Computers*, C-35 (9), pp.803-814, August 1986.

[Boccaletti *et al.* 2006] S. Boccaletti, V. Latora, M. Chavez and D. Hwang, "Complex networks: structure and dynamics", *Physics Reports*, 424, pp.175-308, 2006.

[Bondavalli & Filippini 2004] A. Bondavalli and R. Filippini, "Modeling and Analysis of a Scheduled Maintenance System: a DSPN Approach", *The Computer Journal*, 47 (6), pp.634-650, 2004.

[Bondavalli *et al.* 1999a] A. Bondavalli, I. Majzik and I. Mura, "Automatic Dependability Analysis for supporting design decisions in UML", in *4th IEEE International High Assurance System Engineering Symposium (HASE'99),* (A. Williams, Ed.), IEEE Computer Society Press, 1999a.

[Bondavalli *et al.* 2000] A. Bondavalli, I. Mura, S. Chiaradonna, R. Filippini, S. Poli and F. Sandrini, "DEEM: a tool for the dependability modeling and evaluation of multiple phased systems", in *Int. Conference on Dependable Systems and Networks (DSN2000),* (New York, USA), pp.231-236, IEEE Computer Society, 2000.

[Bondavalli *et al.* 1999b] A. Bondavalli, I. Mura and K. S. Trivedi, "Dependability Modelling and Sensitivity Analysis of Scheduled Maintenance Systems", in *3rd European Dependable Computing Conference (EDCC-3),* (A. Pataricza, J. Hlavicka and E. Maehle, Eds.), (Prague, Czech Republic), pp.7-23, Springer, 1999b.

[Bondavalli *et al.* 2001] A. Bondavalli, M. Nelli, L. Simoncini and G. Mongardi, "Hierarchical Modelling of Complex Control Systems: Dependability Analysis of a Railway Interlocking", *Journal of Computer Systems Science and Engineering*, 16 (4), pp.249-261, 2001.

[Boucherie 1993] R. J. Boucherie, "A characterization of independence for competing Markov chains with application to stochastic Petri nets", in *5th International Workshop on Petri Nets and Performance Models,* (Toulouse, France), pp.117-126, IEEE Computer Society, 1993.

[Brasca *et al.* 2006] C. Brasca, G. Dondossola and F. Garrone, *Control System Scenarios with Interdependencies*, CESI RICERCA S.p.A., October 2006 2006.

[Brocklehurst *et al.* 1994] S. Brocklehurst, T. Olovsson, B. Littlewood and E. Jonsson, "On Measurement of Operational Security", *IEEE Aerospace and Electronics Magazine*, 9 (10) October 1994.

[Bryant 1986] R. E. Bryant, "Graph-based algorithms for Boolean function manipulation", *IEEE Transactions on Computers*, 35, pp.677-691, 1986.

[Bucci & Vicario 1995] G. Bucci and E. Vicario, "Compositional validation of time-critical systems using communicating time Petri nets", *IEEE Transactions on Software Engineering*, 21, pp.969-992, 1995.

[Buchholz 1994] P. Buchholz, "Exact and Ordinary Lumpability in finite Markov Chains", *Journal of Applied Probabilities* (31), pp.59-74, 1994.

[Buchholz 1995a] P. Buchholz, "A Notion of Equivalence for Stochastic Petri Nets", in *16th International Conference on Application and Theory of Petri Nets,* (Torino, Italy), pp.161-180, 1995a.

[Buchholz 1995b] P. Buchholz, "Equivalence relations for stochastic automata networks", in *Computation with Markov Chains* (W. J. Stewart and (ed.), Eds.), Kluwer

Int. Publishers, 1995b.

[Buchholz 1995c] P. Buchholz, "Hierarchical Markovian Models: Symmetries and Reduction", *Performance Evaluation*, 22 (1), pp.93-110, 1995c.

[Buchholz *et al.* 2000] P. Buchholz, G. Ciardo, S. Donatelli and P. Kemper, "Kronecker Operations and Sparse Matrices with Applications to the Solution of Markov Models", *INFORMS Journal on Computing*, 12 (3), pp.203-222, 2000.

[Byres *et al.* 2004] E. J. Byres, M. Franz and D. Miller, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", in *International Infrastructure Survivability Workshop (IISW'04),* (Lisbon, Portugal), 2004.

[CAIDA] CAIDA, *"Home Page of the CAIDA project: http://www.caida.org"*.

[Carreras *et al.* 2002] B. A. Carreras, N. E. Lynch, I. Dobson and D. E. Newman, "Critical Points and Transitions in an Electric Power Transmission Model for Cascading Failure Blackouts", *Chaos*, 12 (4), pp.985-994, 2002.

[Carreras *et al.* 2004a] B. A. Carreras, V. E. Lynch, D. E. Newman and I. Dobson, "Dynamical and Probabilistic Approaches to the Study of Blackout Vulnerability of the Power Transmission Grid", in *37th Hawaii International Conference on System Sciences,* (Hawaii), IEEE Computer Society, 2004a.

[Carreras *et al.* 2004b] B. A. Carreras, D. E. Newman, I. Dobson and B. Poole, "Evidence for Self-Organized Criticality in a Time Series of Electric Power System Blackouts Power Transmission Grid", *IEEE Transactions on Circuits and Systems*, 51 (9), pp.1733-1740, September 2004b.

[CC 2006] CC, *Common Criteria Portal Home page, available online at http://www.commoncriteriaportal.org/, last visited in May 2006*, 2006.

[CCIB 1998] *Common Criteria for Information Technology Security Evaluation - Version 2.0*, Part 1: Introduction and General Model (CCIB-98-026); Part 2: Security Functional Requirements (CCIB-98-027); Part 3: Security Assurance Requirements (CCIB-98-028), Common Criteria Implementation Board, 1998.

[CESI RICERCA 2006a] CESI RICERCA, *Control system scenarios with interdependencies. INPUT to CRUTIAL WP1 rev 0 - Draft*, CESI RICERCA S.p.A., Grid and Infrastructures Department, August 2006a.

[CESI RICERCA 2006b] CESI RICERCA, *Description of Hierarchical Control Schema for the Power Systems and Critical Aspects of their Evaluation. Input to CRUTIAL WP1*, CESI RICERCA S.p.A., Network and Infrastructures Department, May 2006b.

[Chandy *et al.* 1975] K. M. Chandy, U. Herzog and L. Woo, "Parametric Analysis of Queueing Networks", *IBM Journal of Research and Development*, 19 (1), pp.36-42, January 1975.

[Chassin & Posse 2005] D. P. Chassin and C. Posse, "Evaluating North American Electric Grid Reliability Using the Barabasi-Albert Network Model", *Physica A* 2005.

[Chen *et al.* 2002] D. Chen, D. Selvamuthu, D. Chen, L. Li, R. Some, A. P. Nikora and K. S. Trivedi, "Reliability and Availability Analysis for the JPL Remote exploration and Experimentation System ", in *Int Conf. on Dependable Systems and Networks (DSN-02),* pp.337-344, 2002.

[Chen *et al.* 2001] D. Chen, J. S. Thorp and M. Prashar, "Analysis of Electric Power System Disturbance Data", in *34th Hawaii International Conference on System Sciences,* (Hawaii), 2001.

[Chen & Thorp 2002] J. Chen and J. D. Thorp, "A Reliability Study of Transmission System Protection via a Hidden Failure DC Load Flow Model", in *IEEE Fifth International Conference on Power System Management and Control,* pp.384-389, 2002.

[Chen *et al.* 2005] J. Chen, J. D. Thorp and I. Dobson, "Cascading Dynamics and Mitigation Assessment in Power System Disturbances via a Hidden Failure Model", *International Journal of Electrical Power and Electrical Power and Energy Systems* 27 (4), pp.318-326, 2005.

[Chen *et al.* 2006] Q. Chen, C. Jiang, W. Qiu and J. D. McCalley, "Probability Models for Estimating the Probabilities of Cascading Outages in High-Voltage Transmission Network", *IEEE Transactions on Power Systems*, 21 (3), pp.1423-1431, August 2006.

[Chen & McCalley 2004] Q. Chen and J. D. McCalley, "A Cluster Distribution as a Model for Estimating High-Order Event Probabilities in Power Systems", in *8th International Conference on Probabilistic Methods Applied to Power Systems,* (Ames, Iowa, USA), pp.622-628, 2004.

[Chiola *et al.* 1995] G. Chiola, G. Franceschinis, R. Gaeta and M. Ribaudo, "Greatspn 1.7: Graphical editor and analyzer for timed and stochastic Petri nets", *Performance Evaluation*, 24 (1-2), pp.47-68, 1995.

[Choi *et al.* 1994] H. Choi, V. Kulkarni and K. Trivedi, "Markov regenerative stochastic Petri nets. Performance Evaluation", *Performance Evaluation*, 20, pp.337-357, 1994.

[Ciapessoni & Ferrarini 2005] E. Ciapessoni and L. Ferrarini, *Indagine sulla sicurezza funzionale del sistema di automazione delle reti elettriche*, Progetto - NORME, RdS Programme, http://www.ricercadisistema.it/Documenti/SintesiDoc.aspx?idN=1360&idD=312616., December 2005.

[Ciardo 1995] G. Ciardo, "Discrete-time markovian stochastic Petri nets", in *2nd International Workshop on Numerical Solution of Markov Chains,* pp.339-358, 1995.

[Ciardo *et al.* 1994] G. Ciardo, R. German and C. Lindemann, "A characterization of the stochastic process underlying a stochastic Petri net", *IEEE Transactions on Software Engineering*, 20, pp.506-515, 1994.

[Ciardo & Miner 1999] G. Ciardo and A. Miner, "A Data Structure for the Efficient Kroneker Solution of GSPNs", in *8th Int. Workshop on Petri Nets and Performance Models,* (Zaragoza, Spain), pp.22-31, IEEE Computer Society Press, 1999.

[Ciardo & Miner 1996] G. Ciardo and A. S. Miner, "Smart: Simulation and markovian analyzer for reliability and timing", in *IEEE International Computer Performance and Dependability Symposium (IPDS'96),* (Urbana-Champaign, IL, USA), p.60, IEEE Computer Society Society, 1996.

[Ciardo & Trivedi 1993] G. Ciardo and K. S. Trivedi, "Decomposition Approach to Stochastic Reward Net Models", *Performance Evaluation*, 18 (1), pp.37-59, 1993.

[Codetta Raiteri *et al.* 2004] D. Codetta Raiteri, G. Franceschini, M. Iacono and V. Vittorini, "Repairable Fault Tree for the automatic evaluation of repair policies", in *International Conference on Dependable Systems and Networks (DSN '04),* (Florence, Italy), pp.659-668, IEEE Computer Society, 2004.

[Codetta Raiteri *et al.* 2006] D. Codetta Raiteri, G. Franceschinis and M. Gribaudo, "Defining Formalisms and Models in the Draw-Net Modeling System", in *Fourth Workshop on Modelling of Objects, Components and Agents (MOCA2006),* (Turku, Finland), 2006.

[Coleman 1993] J. L. Coleman, "Algorithms for product form stochastic Petri nets - a new approach", in *5th International Workshop on Petri Nets and Performance Models (PNPM-95),* (Toulouse, France), pp.108-116, IEEE Computer Society, 1993.

[Cortelessa & Pompei 2004] V. Cortelessa and A. Pompei, "Towards a UML Profile for QoS: a contribution in the reliability domain", in *4th International Workshop on Software and Performance (WOSP'04),* pp.197-206, 2004.

[Cortelessa *et al.* 2002] V. Cortelessa, H. Singh and B. Cukic, "Early reliability assessment of UML based software models", in *3rd International Workshop on Software and Performance,* (Rome, Italy), pp.302-309, 2002.

[Courtois 1977] P. J. Courtois, *Decomposability - Queueing and Computer System Applications,* ACM Monograph Series, Academic Press, New York, 1977.

[Cox 1955] D. R. Cox, "The Analysis of Non Markovian Stochastic Processes by the Inclusion of Supplementary Variables", *Proc. of the Cambridge Phylosophical Society*, 51, pp.433-440, 1955.

[Crucitti *et al.* 2004a] P. Crucitti, V. Latora and M. Marchiori, "Model for Cascading Failures in Complex Networks", *Physical Review E*, 69 (045104) 2004a.

[Crucitti *et al.* 2003] P. Crucitti, V. Latora, M. Marchiori and A. Rapisarda, "Efficiency of Scale Free Networks: Error and Attack Tolerance of Complex Networks", *Physica A*, 320, pp.622-642, 2003.

[Crucitti *et al.* 2004b] P. Crucitti, V. Latora, M. Marchiori and A. Rapisarda, "Error and Attack Tolerance of Complex Networks", *Physical A*, 340 (1-3), pp.388-394, September 2004b.

[CSEGC 1993] CSEGC, *The Canadian Trusted Computer Evaluation Criteria, Version 3.0e,* Communications Security Establishment Government of Canada, Canadian System Security Centre, 1993.

[Cumani 1985] A. Cumani, "Esp - A package for the evaluation of stochastic Petri nets with phase-type distributed transition times", in *International Workshop Timed Petri Nets,* (Torino, Italy), pp.144-151, IEEE Computer Society, 1985.

[Cuppens & Miege 2002] F. Cuppens and A. Miege, "Alert Correlation in a Cooperative Intrusion Detection Framework", in *2002 IEEE Symposium on Security and Privacy,* (Oakland, CA, USA), pp.202-215, 2002.

[Cymru 2004] Cymru, *"Team Cymru: The Darknet Project. http://www.cymru.com/Darknet",* 2004.

[Dacier & Deswarte 1994] M. Dacier and Y. Deswarte, "The Privilege Graph: an Extension to the Typed Access Matrix Model", in *European Symposium in Computer Security (ESORICS'94),* (D. Gollman, Ed.), (Brighton, UK), Lecture Notes in Computer Science, 875, pp.319-334, Springer-Verlag, 1994.

[Daly 2001] D. Daly, *Analysis of connection as a decomposition technique,* Master Thesis, Univ. of Illinois at Urbana Champaign, Illinois, USA, 2001.

[Daly *et al.* 2004] D. Daly, P. Buchholz and W. H. Sanders, *An approach for bounding Reward Measures in Markov Models Using Aggregation*, Univ. of Illinois at Urbana Champaign, Coordinated Science Lab, July 2004.

[Daly *et al.* 2000] D. Daly, D. D. Deavours, P. G. Webster and W. H. Sanders, "Möbius: An extensible tool for performance and dependability modeling", in *11th International Conference, TOOLS 2000,* (H.

C. B. B. R. Haverkort, and C. U. Smith, Ed.), (Schaumburg, IL, USA), pp.332-336, Lecture Notes in Computer Science, 2000.

[Daly & Sanders 2001] D. Daly and W. H. Sanders, "A connection formalism for the solution of large and stiff models", in *34th Annual Simulation Symposium,* pp.258-265, 2001.

[Delamare *et al.* 2003] C. Delamare, Y. Gardan and P. Moreaux, "Performance evaluation with asynchronously decomposable SWN: implementation and case study", in *10th Int. Workshop on Petri nets and performance models (PNPM03),* (Urbana-Champaign, IL, USA), pp.20-29, IEEE Computer Society Press, 2003.

[Derisavi *et al.* 2003] S. Derisavi, H. Hermanns and W. H. Sanders, "Optimal State space lumping in Markov Chains", *Information Processing Letters*, 87 (6), pp.309-315, 2003.

[Dobson & Carreras 2005] I. Dobson and B. A. Carreras, *Risk Analysis of Critical Loading and Blackouts with Cascading Events*, Consortium for Electric Reliability Technology Solutions (CERTS), 2005, http://eceserv0.ece.wisc.edu/~dobson/home.html.

[Dobson *et al.* 2001] I. Dobson, B. A. Carreras, N. E. Lynch and D. E. Newman, "An initial model for complex dynamics in electric power system blackouts", in *34th Hawaii International Conference on System Sciences (HICSS-34),* (Maui, Hawaii), IEEE Computer Society, 2001, http://eceserv0.ece.wisc.edu/~dobson/home.html.

[Dobson *et al.* 2004a] I. Dobson, B. A. Carreras, V. E. Lynch and D. E. Newman, "Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-organization", in *IREP Symposium on Bulk Power Systems and Control - VI,* (Cortina d'Ampezzo, Italy), pp.438-451, 2004a.

[Dobson *et al.* 2005a] I. Dobson, B. A. Carreras, V. E. Lynch, B. Nkei and D. E. Newman, "A Loading-dependent Model of Probabilistic Cascading Failure", *Probability in the Engineering and Informational Sciences*, 19, pp.475-488, September 2005a.

[Dobson *et al.* 2003] I. Dobson, B. A. Carreras and D. E. Newman, "A Probabilistic Loading-dependent Model of Cascading Failure and Possible Implications for Blackouts", *36th Hawaii International Conference on System Sciences* 2003.

[Dobson *et al.* 2004b] I. Dobson, B. A. Carreras and D. E. Newman, "A Branching Process Approximation to Cascading Load-dependent System Failure", in *37th Hawaii International Conference on System Sciences,* (Hawaii), IEEE Computer Society, 2004b.

[Dobson *et al.* 2005b] I. Dobson, B. A. Carreras and D. E. Newman, "Branching Process Models for the Exponentially Increasing Portions of Cascading Failure Blackouts", in *38th Hawaii International Conference on System Sciences,* (Hawaii), IEEE Computer Society, 2005b.

[Dobson *et al.* 2006] I. Dobson, K. R. Wierzbicki, B. A. Carreras, V. E. Lynch and D. E. Newman, "An Estimator of Propagation of Cascading Failure", in *39th Hawaii International Conference on System Sciences,* (Kauai, Hawaii), IEEE Computer Society, 2006.

[Donatelli 1993] S. Donatelli, "Superposed Stochastic Automata: a class of stochastic Petri nets with parallel solution and distributed state space", *Performance Evaluation*, 18 (1), pp.21-36, 1993.

[Donatelli 1994] S. Donatelli, "Superposed Generalized Stochastic Petri net: definition and efficient solution", in *15th Int. Conf. on Applications and Theory of Petri Nets,* (R. Valette, Ed.), pp.258-277, Springer-Verlag, 1994, Introduction des réseaux de Petri stochastiques généralisés superposés. Présentation du solution basée sur la décomposition et l'algèbre de Kronecker pour leur résolution.

[Donatelli & Franceschinis 1996] S. Donatelli and G. Franceschinis, "The PSR methodology: integrating hardware and software models", in *17th International Conference in Application and Theory of Petri Nets, ICATPN '96,* (Osaka, Japan), Springer-Verlag, 1996.

[Dondossola & Lamquet 2006] G. Dondossola and O. Lamquet, "Cyber Risk Assessment in the Electric Power Industry", *Electra* (224) February 2006.

[Dondossola *et al.* 2004] G. Dondossola, O. Lamquet and M. Masera, *"Emerging standards and methodological issues for the security analysis of the Power System information infrastructures",* Securing critical infrastructures, 2nd International Conference on Critical Infrastructures (CRIS-2004), Grenoble, France, 2004.

[Dorogovtsev & Mendes 2002] S. N. Dorogovtsev and J. F. F. Mendes, "Evolution of networks", *Advances in Physics*, 51, pp.1079-1187, 2002.

[DShield] DShield, *"Home page of the DShield.org Distributed Intrusion Detection System: http://www.dshield.org. "*

[Ealata *et al.* 2005] E. Ealata, M. Dacier, Y. Deswarte, K. Kortchinsky, V. Nicomette and V.-H. Pham, F., "Collection and analysis of attack data based on honeypots deployed on the Internet", in *1st Workshop on Quality of Protection (QOP 2005), (co-located with ESORICS and METRICS),* (F. M. D. Gollmann, A. Yautsiukhin, Ed.), (Milan, Italy), pp.79-92, Springer, 2005.

[Fink & Carlsen 1978] L. H. Fink and K. Carlsen, "Operating Under Stress and Strain", *IEEE Spectrum* (March), pp.48-53, 1978.

[Fota *et al.* 1999] N. Fota, M. Kâaniche and K. Kanoun, "Incremental Approach for Building Stochastic Petri Nets for Dependability Modeling", in *Statistical and Probabilistic Models in Reliability* (D. C. Ionescu and N. Limnios, Eds.), pp.321-335, Birkhäuser, 1999.

[Franceschinis *et al.* 2002] G. Franceschinis, M. Gribaudo, M. Iacono, N. Mazzocca and V. Vittorini, "Drawnet++: Model objects to support performance analysis and simulation of complex systems", in *Lecture Notes in Computer Science* LNCS 2324, pp.233-238, Springer-Verlag, 2002.

[Fricks *et al.* 1997] R. Fricks, C. Hirel, S. Wells and K. Trivedi, "The development of an integrated modeling environment", in *World Congress on Systems Simulation (WCSS '97),* (Singapore), pp.471-476, 1997.

[Gao 2004] Gao, *Critical Infrastructure Protections: Challenges and Efforts to Secure Control Systems*, Government Accountability Office, N°GAO-04-354, 2004, www.gao.gov/new.items/d04354.pdf.

[Garetto *et al.* 2003] M. Garetto, W. Gong and D. Towsley, "Modeling Malware Spreading Dynamics", in *INFOCOM'2003,* (San Francisco, CA, USA), 2003.

[German *et al.* 1995a] R. German, C. Kelling, A. Zimmermann and G. Hommel, "Timenet: A toolkit for evaluating non-markovian stochastic petri-nets", *Performance Evaluation*, 24, pp.69-87, 1995a.

[German & Lindemann 1994] R. German and C. Lindemann, "Analysis of Stochastic Petri Nets by the Method of Supplementary Variables", *Performance Evaluation*, 20, pp.317-335, 1994.

[German *et al.* 1995b] R. German, D. Logothetis and K. Trivedi, "Transient analysis of Markov Regenerative Stochastic Petri Nets: a comparison of approaches", *6-th International Conference on Petri Nets and Performance Models (PNPM95)*, pp.103-112, 1995b.

[Gribaudo & Horváth 2002] M. Gribaudo and A. Horváth, "Fluid stochastic petri nets augmented with flush-out arcs: A transient analysis technique", *IEEE Transactions On Software Engineering*, 28 (10), pp.944-955, 2002.

[Gribaudo *et al.* 2003] M. Gribaudo, A. Horváth, A. Bobbio, E. Tronci, E. Ciancamerla and M. Minichino, "Fluid Petri nets and hybrid model-checking: A comparative case study", *Reliability Engineering & System Safety*, 81 (3), pp.239-257, 2003.

[Gribaudo *et al.* 2005] M. Gribaudo, N. Mazzocca, F. Moscato and V. Vittorini, "Multisolution of Complex Performability Models in the OsMoSys/DrawNet Framework

", in *2nd Int. Conf. on the Quantitative Evaluation of Systems (QEST2005),* (Torino, Italy), pp.85-94, IEEE Computer Society Press, 2005.

[Gribaudo & Sereno 2000] M. Gribaudo and M. Sereno, "Simulation of Fluid Stochastic Petri Nets", in *Eighth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2000)* (San Francisco, CA,USA), pp.231-239, 2000.

[Gribaudo *et al.* 2001] M. Gribaudo, M. Sereno, A. Horváth and A. Bobbio, "Fluid stochastic Petri nets augmented with flush-out arcs: Modelling and analysis", *Discrete Event Dynamic Systems*, 11 (1-2), pp.97-117, January 2001.

[Gupta *et al.* 2003] V. Gupta, V. V. Lam, H. V. Ramasamy, W. H. Sanders and S. Singh, "Dependability and Performance Evaluation of Intrusion Tolerant-Server Architectures", in *First Latin-American Symposium on Dependable Computing (LADC 2003),* (Sao-Paulo, Brazil), pp.81-101, IEEE Computer Society, 2003.

[Haddad & Moreaux 1995] S. Haddad and P. Moreaux, "Evaluation of High-level Petri nets by means of aggregation and decomposition", in *Sixth International Workshop on Petri Nets and Performance Models,* (Durham, NC, USA.), pp.11-20, IEEE Computer Society Press 1995.

[Haddad & Moreaux 1996] S. Haddad and P. Moreaux, "Asynchronous Composition of High-level Petri nets : a quantitative approach", in *17th International Conference on Application and Theory of Petri nets,* (Osaka, Japan), pp.192-211, 1996.

[Haddad & Moreaux 2004] S. Haddad and P. Moreaux, "Approximate Analysis of Non-Markovian Stochastic Systems with Multiple Time Scale Delays", in *12th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)* (Volendam, The Netherlands), 2004.

[Haddad *et al.* 2005] S. Haddad, P. Moreaux, M. Sereno and M. Silva, "Product-form and stochastic Petri nets: a structural approach", *Performance Evaluation*, 59, pp.313-336, 2005.

[Hardy *et al.* 2005] G. Hardy, C. Lucet and N. Limnios, "Computing all-terminal reliability of stochastic networks by Binary Decision Diagrams", in *Applied Stochastic Modeling and Data Analysis (ASMDA'2005),* 2005.

[Heckermann *et al.* 1995] D. Heckermann, Wellman and Mandani, "Real-world applications of Bayesian Networks", *Communications of the ACM*, 38 (3) 1995.

[Heindl & German 1997] A. Heindl and R. German, "A fourth-order algorithm with automatic stepsize control for the transient analysis of DSPNs", in *7-th International Conference on Petri Nets and Performance Models (PNPM'97),* pp.60-69, IEEE Computer Society, 1997.

[Henderson *et al.* 1989] W. Henderson, D. Lucic and P. G. Taylor, "A net level performance analysis of stochastic Petri nets", *Journal of Australian Mathematical Society*, Ser. B (31), pp.176-187, 1989.

[Henzinger *et al.* 1995] T. A. Henzinger, P.-H. Ho and H. Wong-Toi, "A user guide to HyTech", in *1st Workshop Tools and Algorithms for the Construction and Analysis of Systems (TACAS),* pp.41-71, Springer Verlag, 1995.

[Hines *et al.* 2006] P. Hines, J. Apt, H. Liao and S. N. Talukdar, "The Frequency of Large Blackouts in the United States Electrical Transmisson System: An Empirical Study", in *2nd Annual Carnegie Mellon University Conferenec on Electric Power Systems: Monitoring, Sensing, Software and Its Valuation for the Changing Electric Power Industry,* (Carnegie Mellon, USA), 2006, http://www.ece.cmu.edu/~electricityconference/hines_blackout_frequencies_final.pdf.

[HiQPN] HiQPN, *"The HiQPN Software.web link: http://ls4-www.informatik.uni-dortmund.de/QPN."*

[Horton *et al.* 1998] G. Horton, V. Kulkarni, D. M. Nicol and K. Trivedi, "Fluid stochastic Petri nets: Theory, application and solution techniques", *European Journal of Operational Research*, 105 (1), pp.184-201, 1998.

[Horváth 2005] A. Horváth, "Steady state solution for models with geometric and finite support activity duration", in *2nd International Conference on the Quantitative Evaluation of Systems (QEST),* (Torino, Italy), 2005.

[Horváth & Gribaudo 2002] A. Horváth and M. Gribaudo, "Matrix geometric solution of fluid stochastic petri nets", in *4th International Conference on Matrix-Analytic Methods in Stochastic models,* (Adelaide, Australia), 2002.

[Howard 1960] R. A. Howard, *Dynamic Probabilistic Systems and Markov Models,* 576p., the MIT Press, 1960.

[Illié *et al.* 2004] J. M. Illié, S. Baarir, M. Beccuti, C. Delamare, S. Donatelli, C. Dutheillet, G. Franceschinis, R. Gaeta and P. Moreaux, "Extended SWN solvers in GreatSPN", in *1st International Conference on Quantitative Evaluation of Systems (QEST),* (Enschede, The Netherlands), IEEE Computer Society Press, 2004.

[ITSEC 1991] ITSEC, *Information Technology Security Evaluation Criteria*, Office for Official Publications of the European Communities, June 1991.

[Jacobson & Lazowska 1981] P. A. Jacobson and E. D. Lazowska, "The Method of Surrogate Delays: Simultaneous Resource Possession in Analytic Models of Computer Systems", in *The ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems,* (Las Vegas, USA), pp.165-174, 1981.

[Jajodia *et al.* 2003] S. Jajodia, S. Noel and B. O'Berry, "Topological Analysis of Network Attack Vulnerability ", in *Managing Cyber Threats: Issues, Approaches and Challenges* (S. S. V. Kumar, A. Lazarevic, Ed.), Kluwer Academic Publisher, 2003, 2003.

[JCSEC 1992] JCSEC, *The Japanese Computer Security Evaluation Criteria - Functionality Requirements, Draft V 1.0*, Ministry of International Trade and Industry, 1992.

[Jonsson & Olovsson 1997] E. Jonsson and T. Olovsson, "A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior", *IEEE Transactions on Software Engineering*, 23 (4), pp.235-245, April 1997.

[Jungnitz & Desrochers 1991] H. Jungnitz and A. Desrochers, "Flow equivalent nets for the performance analysis of flexible manufacturing systems", in *1991 IEEE Robotics and Automation Conference,* pp.122-127, 1991.

[Kaâniche *et al.* 2006] M. Kaâniche, E. Alata, V. Nicomette, Y. Deswarte and M. Dacier, "Empirical Analysis and Statistical Modeling of Attack Processes based on Honeypots", in *WEEDS 2006 - workshop on empirical evaluation of dependability and security (in conjunction with the international conference on dependable systems and networks, (DSN2006),* pp.119-124, 2006.

[Kaâniche *et al.* 2003] M. Kaâniche, K. Kanoun and M. Rabah, "Multi-level modelling approach for the availability assessment of e-business applications", *Software: Practice and Experience*, 33 (14), pp.1323-1341, 2003.

[Kanoun & Borrel 2000] K. Kanoun and M. Borrel, "Fault-Tolerant System Dependability — Explicit Modeling of Hardware and Software Component-Interactions", *IEEE Transactions on Reliability*, 49 (4), pp.363-376, December 2000.

[Kanoun *et al.* 1999] K. Kanoun, M. Borrel, T. Moreteveille and A. Peytavin, "Modeling the Dependability of CAUTRA, a Subset of the French Air Traffic Control System", *IEEE Transactions on Computers*, 48 (5), pp.528-535, 1999.

[Kemeny & Snell 1959] J. G. Kemeny and J. L. Snell, *Finite Markov Chains,* Princeton, NJ: Van Nostrand, 1959.

[Kemper 1996] P. Kemper, "Numerical analysis of superposed GSPNs", *IEEE Transactions on Software Engineering*, 22 (4), pp.615-628, 1996.

[Kinney *et al.* 2005] R. Kinney, P. Crucitti, R. Albert and V. Latora, "Modeling Cascading Failures in the North American Power Grid", *The European Physical Journal B*, 46 (1), pp.101-107, 2005.

[Krings & Oman 2003] A. Krings and P. Oman, "A simple GSPN for modeling common-mode failures in critical infrastructures", in *36th Hawai Int. Conf. on System Sciences,* p.10, 2003.

[Kwiatkowska & Sproston 2003] M. Kwiatkowska and J. Sproston, "Probabilistic Model Checking of Deadline Propeties in the IEEE 1394 FireWire Protocol", *Formal Aspects of Computing*, 14 (3), pp.295-318, 2003.

[Lanus *et al.* 2003] M. Lanus, L. Yin and K. S. Trivedi, "Hierarchical Composition and Aggregation of State-based Availability and Performability Models", *IEEE Transactions on Reliability*, 52 (1), pp.44-52, 2003.

[Lazar & Robertazzi 1987] A. A. Lazar and T. G. Robertazzi, "Markovian Petri net protocols with product form solution", in *IEEE INFOCOM '87,* (San Francisco, CA., USA), pp.1054-1062, 1987.

[Lee *et al.* 2004] E. E. Lee, J. E. Mitchell and W. A. Wallace, *"Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems",* 37th Hawaii International Conference on System Sciences, IEEE Computer Society, Hawaii, 2004.

[Leurré.com] Leurré.com, *"Leurré.com project. Publications web page : http://www.leurrecom.org/paper.htm"*.

[Leuven 2006] K. U. Leuven, *Description of a Distributed Control Scheme for Distributed Generation*, K.U. Leuven, ESAT/ELECTA April 2006 2006.

[Lindemann *et al.* 1999] C. Lindemann, A. Reuys and A. Thümmler, "The dspnexpress 2.000 performance and dependability modeling environment", in *29th Annual Int. Symp. on Fault-Tolerant Computing (FTCS-29),* (Madison, Wisconsin, USA), pp.228-231, IEEE Computer Society, 1999.

[Littlewood *et al.* 1993] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, J. McDermid and D. Gollmann, "Towards Operational Measures of Computer Security", *Journal of Computer Security*, 2, pp.211-229, 1993.

[Lollini 2005] P. Lollini, *On the modelling and solution of complex systems: from two domain-specific case-studies towards the definition of a more general framework,* PhD, University of Florence, Italy, December 2005, http://rcl.dsi.unifi.it/theses/TesiLollini.pdf

[Lollini *et al.* 2005] P. Lollini, A. Bondavalli and F. Di Giandomenico, "A modeling methodology for hierarchical control systems and its application", *Journal of the Brazilian Computer Society*, 10 (3), pp.57-69, 2005.

[Luo & Trivedi 1998] T. Luo and K. Trivedi, "An improved algorithm for coherent-system reliability, IEEE Transactions on Reliability, 47, 73-78, 1998", *IEEE Transactions on Reliability*, 47, pp.73-78, 1998.

[Lye & Wing 2005] K.-w. Lye and J. M. Wing, "Game strategies in network security", *International Journal on Information Security*, 4 (1-2), pp.71-86, 2005.

[Madan *et al.* 2002] B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan and K. Trivedi, "Modeling and Quantification of Security Attributes of Software Systems", in *IEEE International Conference on Dependable Systems and Networks (DSN 2002),* (Wahsington, DC, USA), pp.505-514, IEEE computer Society, 2002.

[Majzik *et al.* 2003] I. Majzik, A. Pataricza and A. Bondavalli, "Stochastic Dependability Analysis of System Architecture Based on UML Models", in *Architecting Dependable Systems* (C. G. R. De Lemos, and A. Romanovsky, Ed.), LNCS 2677, pp.219-244, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

[Marie 1979] R. Marie, "An approximate analytical method for general queueing networks", *IEEE Transaction on Software engineering*, SE-5, pp.530-538, 1979.

[Masera 2002] M. Masera, *"An Approach to the Understanding of Interdependencies",* Power Systems and Communications Infrastructures for the Future (CRIS'2002), Beijing, China, 2002.

[Merlin & Faber 1976] P. M. Merlin and D. J. Faber, "Recoverability of communication protocols - Implication of a theoretical study", *IEEE Transactions on Communication*, 24, pp.1036-1043, 1976.

[Meyer & Sanders 1993] J. F. Meyer and W. H. Sanders, "Specification and Construction of Performability Models", in *Int. Workshop on Performability Modeling of Computer and Communication Systems,* (Mont Saint Michel, France), pp.1-32, 1993.

[Milner 1989] R. Milner, *Communication and Concurrency,* Prentice Hall, 1989.

[Miner & Parker 2004] A. S. Miner and D. Parker, "Symbolic Representations and Analysis of large probabilistic systems", in *Validation of Stochastic Systems* LNCS 2925, Springer, 2004.

[Montani *et al.* 2005] S. Montani, L. Portinale and A. Bobbio, "Dynamic bayesian networks for modeling advanced fault tree features in dependability analysis", in *Proc. ESREL 2005,* (Tri City), p.June, 2005.

[Motter & Lai 2002] A. E. Motter and Y. C. Lai, "Cascade-based Attacks on Complex Networks", *Physics Review E*, 66 (065102) 2002.

[Muppala *et al.* 1992] J. K. Muppala, A. Sathaye, R. Howe and K. S. Trivedi, "Dependability Modeling of a Heterogeneous VAX-cluster System Using Stochastic Reward Nets", in *Hardware and Software Fault Tolerance in Parallel Computing Systems* (D. R. Avresky, Ed.), pp.33-59, 1992.

[Mura & Bondavalli 2001] I. Mura and A. Bondavalli, "Markov Regenerative Stochastic Petri Nets to Model and Evaluate the Dependability of Phased Missions", *IEEE Transactions on Computers*, 50 (12), pp.1337-1351, 2001.

[Mura *et al.* 1999] I. Mura, A. Bondavalli, X. Zang and K. Trivedi, "Dependability Modelling and Evaluation of Phased Mission Systems: a DSPN Approach", in *7th IFIP Int. Conference on Dependable Computing for Critical Applications (DCCA-7),* (San Jose, CA, USA), IEEE Computer Society, 1999.

[Nedic 2003] D. P. Nedic, *Simulation of Large System Disturbances,* PhD, The University of Manchester -UMIST, Manchester, United Kingdom, 2003.

[Nelli *et al.* 1996] M. Nelli, A. Bondavalli and L. Simoncini, "Dependability Modelling and Analysis of Complex Control Systems: an Application to Railway Interlocking", in *European Dependable Computing Conference (EDCC-2),* (Taormina, Italy), pp.93-110, Springer-Verlag, 1996.

[NERC] NERC, *Information on Blackouts in North America, Disturbance Analysis Working Group (DAWG)*, http://www.nerc.com/~dawg/databas.html.

[Newman 2003] M. E. Newman, "The structure and function of complex networks", *SIAM Review*, 45 (167-256) 2003.

[Nicol *et al.* 2004] D. M. Nicol, W. H. Sanders and K. S. Trivedi, "Model-based Evaluation: From Dependability to Security", *IEEE Transactions on Dependable and Secure Computing,*, 1 (1), pp.48-65, 2004.

[Ning *et al.* 2002] P. Ning, Y. Cui and D. S. Reeves, "Constructing Attack Scenarios Through Correlation of Intrusion Alerts", in *9th ACM Conference on Computer and Communication Security (CCS'02),* (Washington DC, USA), pp.245-254, 2002.

[Obal 1998] W. D. Obal, *Measure-Adaptive State-Space Construction Methods,* PhD, University of Arizona, 1998.

[Ortalo *et al.* 1999] R. Ortalo, Y. Deswarte and M. Kaâniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security", *IEEE Transactions on Software Engineering*, 25 (5), pp.633-650, 1999.

[Page & Perry 1988] L. B. Page and J. E. Perry, "A practical implementation of the factoring theorem for network reliability", *A practical implementation of the factoring theorem for network reliability*, 37, pp.259-267, 1988.

[Pederson *et al.* 2006] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory, USA, August 2006.

[Phillips & Swiler 1998] C. Phillips and L. Swiler, "A Graph-based System for Network Vulnerability Analysis", in *New Security Paradigm Workshop,* (Charlottesville, VA, USA), 1998.

[Plateau 1985] B. Plateau, "On the stochastic structure of parallelism and synchronisation models for distributed algorithms", in *1985 ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems,* (Austin, TX, USA), pp.147-153, 1985.

[Pooley 1991] R. J. Pooley, "The integrated modelling support environment: A new generation of performance modelling tools", in *5th International Conference in Computer Performance Evaluation: Modelling Techniques and Tools,* (G. B. a. G. Serazzi, Ed.), (Torino, Italy), pp.1-15, 1991.

[Pothamsetty & Franz 2005] V. Pothamsetty and M. Franz, *"SCADA HoneyNet Project: Building Honeypots for Industrial Networks (http://scadahoneynet.sourceforge.net/)",* (November 2006), 2005.

[Pourbeik *et al.* 2006] P. Pourbeik, P. S. Kundur and C. W. Taylor, "The Anatomy of a Power Grid Blackout", *IEEE Power & Energy Magazine* (September/october), pp.22-29, 2006.

[Puterman 2005] M. L. Puterman, *Markov Decision Processes. Discrete Stochastic Dynamic Programming,* Wiley, 2005.

[Rabah & Kanoun 2003] M. Rabah and K. Kanoun, "Performability evaluation of multipurpose multiprocessor systems: the "separation of concerns" approach", *IEEE transactions on Computers*, 52 (2), pp.223-236, 2003.

[Rahman & Besnosov 2006] H. A. Rahman and K. Besnosov, "Identification of sources of failures and their propgation in critical infrastructures from 12 Years of public failure reports", in *CRIS'2006, Third International Conference on critical Infrastructures,* (Allessandria, VA, USA), 2006.

[Rinaldi 2004] S. M. Rinaldi, *"Modeling and Simulating Critical Infrastructures and Their Interdependencies",* 37th Hawaii International Conference on System Sciences, (5-8 January), IEEE Computer Society, Hawaii, 2004.

[Rinaldi *et al.* 2001] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine* (December), pp.11-25, 2001.

[Rios *et al.* 2002] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic and R. N. Allan, "Value of security: Modeling time- dependent phenomena and weather conditions", *IEEE Transactions on Power Systems*, 17 (3), pp.543-548, 2002.

[Rojas 1996] I. Rojas, "Compositional Construction of SWN Models", *The Computer Journal*, 38 (7), pp.612-621, 1996.

[Rugina *et al.* 2006] A. E. Rugina, K. Kanoun and M. Kaâniche, "An architecture-based dependability modeling framework using AADL ", in *10th IASTED International Conference on Software Engineering and Applications (SEA'2006),* (Dallas, USA), pp.222-225, 2006.

[Sahner *et al.* 1996] R. A. Sahner, K. Trivedi and A. Puliafito, *Performance and Reliability Analysis of Computer Systems: An Example-based Approach Using the SHARPE Software Package,* 404p., Kluwer Academic Publisher, 1996.

[Sahner & Trivedi 1987] R. A. Sahner and K. S. Trivedi, "Reliability modeling using SHARPE", *IEEE Transactions on Reliability*, R-36 (2), pp.186-193, 1987.

[Sallhammar *et al.* 2006] K. Sallhammar, B. E. Helvik and S. J. Knapskog, "A Game-theoretic Approach to Stochastic Security and Dependability Evaluation", in *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06),* (Indianapolis, USA), 2006.

[Sallhammar *et al.* 2005] K. Sallhammar, S. J. Knapskog and B. E. Helvik, "Using Stochastic Game Theory to Compute the Expected Behavior of Attackers", in *The 2005 Symposium on Applications and the Internet Workshops (SAINT-W'05),* pp.102-105, 2005.

[Sanders 1999] W. H. Sanders, "Integrated frameworks for multi-level and multi-formalism modeling", in *8th International Workshop on Petri Nets and Performance Models (PNPM'99),* (Saragoza, Spain), pp.2-9, 1999.

[Sanders & Meyer 2001] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: Formal definitions and concepts", in *Lectures on Formal Methods and Performance Analysis. Lecture Notes in Computer Science* 2090, pp.315-343, Springer-Verlag, 2001.

[Sanders *et al.* 1995] W. H. Sanders, W. D. Obal II, M. A. Qureshi and F. K. Widjanarko, "The *UltraSAN* Modeling Environment", *Performance Evaluation*, 21 (special "Performance Evaluation Tools") 1995.

[Scarpa & Bobbio 1998] M. Scarpa and A. Bobbio, "Kronecker representation of stochastic Petri nets with discrete PH distributions", in *International Computer Performance and Dependability Symposium (IPDS'98),* (Durham, NC, USA), pp.52-61, IEEE Computer Society Press, 1998.

[Schainker *et al.* 2006] R. Schainker, J. Douglas and T. Kropp, "Electric Utility Reponses to Grid Security Issues", *IEEE Power & Energy Magazine* (March/April), pp.30-37, 2006.

[Schneier 1999] B. Schneier, "Modeling Security Threats", *Mr Dobb's Journal* December 1999.

[Sereno & Balbo 1993] M. Sereno and G. Balbo, "Computational Algorithms for Product Form Soultion Stochastic Petri Nets", in *5th International Workshop on Petri Nets and Performance Models (PNPM-95),* (Toulouse, France), pp.98-107, IEEE Computer Society, 1993.

[Sheyner *et al.* 2002] O. Sheyner, J. Haines, S. Jha, R. Lippmann and J. M. Wing, "Automated Generation and Analysis of Attack Graphs", in *2002 IEEE Symposium on Security and Privacy, Oakland, CA, USA,* 2002.

[Song *et al.* 2000] H. Song, C.-C. Liu and R. W. Dahlgren, "Optimal Electricity Supply Bidding by Markov Decision Processes", *IEEE Transactions on Power Systems*, 15 (2), pp.618-624, 2000.

[Staniford *et al.* 2002] S. Staniford, V. Pawson and N. Weaver, "How to Own the Internet in your Spare Time", in *USENIX Security Symposium,* pp.149-167, 2002.

[Sun 2005] K. Sun, "Complex Networks Theory: A New Method of Research in Power Grid", in *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES,* (Dalian, China), pp.1-6, 2005.

[Talukdar *et al.* 2003] S. N. Talukdar, J. Apt, M. Ilic, L. B. Lave and M. G. Morgan, "Cascading Failures: Survival versus Prevention", *The Electricity Journal* November 2003.

[TCSEC 1985] TCSEC, *Trusted Computer System Evaluation Criteria*, Department of Defense, USA, 1985.

[Thorp *et al.* 1998] J. D. Thorp, A. G. Phadke, S. H. Horowitz and S. Tamronglak, "Anatomy of Power System Disturbances: Importance Sampling", *Electric Power and Energy Systems*, 20 (2), pp.147-152, 1998.

[Trivedi 2002] K. Trivedi, "Sharpe 2002: symbolic hierarchical automated reliability and performance evaluator", in *IEEE Int. Conference on Dependable Systems and Networks (DSN 2002),* (Washington, DC, USA), p.544, IEEE Computer Society, 2002.

[Trivedi & Kulkarni 1993] K. Trivedi and V. Kulkarni, "FSPNs: Fluid Stochastic Petri Nets", in *International Conference on Application and Theory of Petri Nets (ICATPN-93),* pp.24-31, Springer-Verlag, 1993.

[Tuffin *et al.* 2001] B. Tuffin, D. S. Chen and K. Trivedi, "Comparison of hybrid systems and fluid stochastic Petri nets", *Discrete Event Dynamic Systems*, 11 (1-2), pp.77-95, January 2001.

[US-Canada 2004] US-Canada, *Power System Outage Task Force — Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004 2004.

[van Moorsel & Huang 1998] A. P. A. van Moorsel and Y. Huang, "Reusable software components for performability tools, and their utilization for web-based configuration tools", in *10th International Conference in Computer Performance Evaluation: Modelling Techniques and Tools,* (N. N. S. R. Puigjaner, and B. Serra, Ed.), (Palma de Mallorca, Spain), pp.37-50, 1998.

[Vicario 2001] E. Vicario, "Static analysis and dynamic steering of time dependent systems", *IEEE Transactions on Software Engineering*, 27 (8), pp.728-748, 2001.

[Wang *et al.* 2003] D. Wang, B. B. Madan and K. Trivedi, "Security Analysis of SITAR Intrusion-Tolerant System", in *ACM Workshop Survivable and Self-Regenerative Systems,* pp.23-32, 2003.

[Watts 2002] Watts, D.J., "A Simple Model of Global Cascades on Random Networks", *Proceedings of the National Academy of Science USA*, 99, pp.5766-5771, 2002.

[Wenger *et al.* 2004] A. Wenger, J. Metzger, M. Dunn and I. Wigert, *Critical Information Infrastructure Protection — International CIIP Handbook 2004*, ETH the Swiss Federal Institute of Technology, 2004.

[Weron & Simonsen 2006] R. Weron and I. Simonsen, "Blackouts, risk and Fat-tailed Distributions", in *Practical Fruits of Econophysics* (H. Takayasu, Ed.), pp.215-219, Springer-Tokyo, Tokyo, 2006.

[Woodside *et al.* 1995] C. M. Woodside, J. E. Neilson, D. C. Petriu and S. Mahumdar, "The Stochastic Rendezvous Network Model for Performance of Synchronous Client-Server-like Distributed Software", *IEEE Transactions on Computers*, 44 (1), pp.20-34, 1995.

[Zaho *et al.* 2004] L. Zaho, K. Park and Y. C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown", *Physical Review E*, 70 (035101), pp.1-4, 2004.

[Zou *et al.* 2002] C. C. Zou, W. Gong and D. Towsley, "Code Red Worm Propagation Modeling and Analysis", in *ACM Conference on Computer and Communications Security CCS'02,* (Washington DC, USA), 2002.

[Zou *et al.* 2005] C. C. Zou, W. Gong, D. Towsley and L. Gao, "The Monitoring and Early Detection of Internet Worms", *IEEE/ACM Transactions on Networking*, 13 (5), pp.961-974, October 2005.