# Reliability engineering: Old problems and new challenges

Enrico Zio

# RELIABILITY ENGINEERING: OLD PROBLEMS AND NEW CHALLENGES

E. Zio
*Dept. of Energy, Polytechnic of Milan, Via Ponzio 34/3, 20133 Milan, Italy*
*Phone: +39-2-2399-6340; fax: +39-2-2399-6309*
*E-mail address: enrico.zio@polimi.it*

## Abstract

*The first recorded usage of the word reliability dates back to the 1800s, albeit referred to a person and not a technical system. Since then, the concept of reliability has become a pervasive attribute worth of both qualitative and quantitative connotations. In particular, the revolutionary social, cultural and technological changes that have occurred from the 1800s to the 2000s have contributed to the need for a rational framework and quantitative treatment of the reliability of engineered systems and plants. This has led to the rise of reliability engineering as a scientific discipline.*

*In this paper, some considerations are shared with respect to a number of problems and challenges which researchers and practitioners in reliability engineering are facing when analyzing today's complex systems. The focus will be on the contribution of reliability to system safety and on its role within system risk analysis.*

**Keywords:** Reliability engineering, Safety, Risk Analysis, Uncertainty, Complex Systems

# 1 Introduction

This paper collects a number of considerations on problems and challenges of current reliability engineering research, that were shared during the keynote lecture by the author at the European Safety and Reliability Conference ESREL 2007 held in Stavanger (Norway) in 2007. The focus on reliability engineering is with respect to its role within the current developments of system safety and risk analysis. The focus on the problems and challenges relates to the representation and modeling of the complexity of the systems, to the quantification of the system models and to the proper representation, propagation and quantification of the uncertainty in the system failure behavior and model. The focus on the research for techniques and methods to address such problems and challenges is strongly biased towards the new computational developments continuously stimulated by the constantly increasing computing power and capabilities.

The author apologizes at the forefront for the incapability of treating the subject exhaustively, with the deserved completeness of material and references and with the due profundity: seeking such objectives would have rendered overwhelming the task of writing the paper… as well as that of reading it.

Reliability is a fundamental attribute for the safe operation of any modern technological system. Focusing on safety, reliability analysis aims at the quantification of the probability of failure of the system and its protective barriers. In practice, diverse types of protection barriers are placed as safeguards from the hazard posed by the system operation, within a *multiple-barrier* concept. These barriers are intended to protect the system from failures of any of its components, hardware, software, human and organizational. These all need to be addressed by the system reliability analysis in a comprehensive and integrated manner (Reason, 1998).

A fundamental issue in reliability analysis is the uncertainty in the failure occurrences and consequences. For the objectives of system safety, this entails protecting the system beyond the uncertainties of its accidental scenarios.

One classical way to defend a system beyond the uncertainty of its failure scenarios has been to: i) identify the group of failure event sequences leading to credible *worst-case* accident scenarios $\{s^*\}$ (*design-basis accidents*), ii) predict their consequences $\{x^*\}$ and iii) accordingly design proper safety barriers for preventing such scenarios and for protecting from, and mitigating, their associated consequences.

Within this *structuralist, defense-in-depth* approach, safety margins against these scenarios are enforced through conservative regulations of system design and operation, under the creed that the identified worst-case, credible accidents would envelope all credible accidents for what regards the

challenges and stresses posed on the system and its protections. The underlying principle has been that if a system is designed to withstand all the worst-case credible accidents, then it is 'by definition' protected against any credible accident (Apostolakis, 2006a).

This approach has been the one classically undertaken, and in many technological instances it still is, to protect a system from the uncertainty of the unknown failure behaviours of its components, systems and structures, without directly quantifying it, so as to provide reasonable assurance that the system can be operated without undue risk. However, the practice of referring to "worst" cases implies subjectivity and arbitrariness in the definition of the accidental events, which may lead to the consideration of scenarios characterized by really catastrophic consequences, although highly unlikely. This may lead to the imposition of unnecessarily stringent regulatory burdens and thus excessive conservatism in the design and operation of the system and its protective barriers, with a penalization of the industry. This is particularly so for those industries, such as the nuclear, aerospace and process ones, in which accidents may lead to potentially large consequences.

For this reason, a more rational and quantitative approach has been pushed forward for the design, regulation and management of the safety of hazardous systems. This approach, initially motivated by the growing use of nuclear energy and by the growing investments in aerospace missions in the 1960s, stands on the principle of looking quantitatively also at the reliability of the accident-preventing and consequence-limiting protection systems which intervene in all potential accident scenarios, in principle with no longer any differentiation between credible and incredible, large and small accidents (Farmer, 1964). Initially, a number of studies were performed for investigating the merits of a quantitative approach based on probability for the treatment of the uncertainty associated with the occurrence and evolution of accident scenarios (Garrick et al., 1967). The findings of these studies motivated the first complete and full-scale probabilistic risk assessment of a nuclear power installation (WASH-1400, 1975). This extensive work showed that indeed the dominant contributors to risk need not be necessarily the design-basis accidents, a 'revolutionary' discovery undermining the fundamental creed underpinning the structuralist, defense-in-depth approach to safety (Apostolakis, 2006a).

Following these lines of thought, and after several 'battles' for their demonstration and valorisation, the probabilistic approach to risk analysis (PRA) has arisen as an effective way for analysing system safety, not limited only to the consideration of worst-case accident scenarios but extended to looking at all feasible scenarios and its related consequences, with the probability of occurrence of such scenarios becoming an additional key aspect to be quantified in order to rationally and quantitatively handle uncertainty (WASH-1400, 1975; NASA, 2002; Aven, 2003; Bedford and Cooke, 2001; Henley and Kumamoto, 1992; Kaplan and Garrick, 1984; McCormick, 1981;

NUREG, 1983). From the view point of safety regulations, this has led to the introduction of new criteria which account for both the consequences of the scenarios and their probabilities of occurrence under a now *rationalist*, defense-in-depth approach. Within this approach to safety analysis and regulation, reliability engineering takes on a most relevant role in the assessment of the probability of occurrence of the accident scenarios.

In the next Section, the historic evolution of reliability engineering is briefly re-visited, highlighting some of the major achievements and transformations occurred through the years. This paves the way for the presentation of the current issues and challenges that reliability engineering is facing today. In Section 3.1, these are focused on the representation and modeling of the complexity of the system and all its components, hardware, software, human and organizational. The modeling and computational challenges thereby arising are discussed with reference to some of the current research developments in computational methodologies and techniques for their solution. Exemplary cases of complexity, which are discussed in some details, are the multi-state systems and the network systems which typically make up the modern infrastructures of distributed service (e.g. computer and communication systems, electric power transmission and distribution systems, rail and road transportation systems, water/oil/gas distribution systems). In Section 3.2, the focus is on the current issues and challenges faced for maintaining a system or structure at the desired level of reliability and performance during its operation life. The discussion thus touches upon the problems related to the maintenance of complex systems and structures, with its associated challenges of diagnosing and predicting the failure behavior of its components with due account of the associated uncertainties. The fundamental issue of the proper representation and modeling of uncertainty is discussed in Section 3.3, where a number of alternative mathematical frameworks of uncertainty representation are mentioned under a set of common objectives for their practical use for rational safety and reliability decision making. Section 4 represents a shy daring into some seemingly evident needs in the practice of reliability engineering. Finally, Section 5 wraps up some of the issues touched upon under a modern, dynamic view of reliability engineering for system safety.

# 2 Reliability engineering from yesterday to today

It seems that the word *reliability* was first coined by the English poet Samuel T. Coleridge, who along with William Wordsworth started the English Romantic Movement (Engell et al., 1983):

*"He inflicts none of those small pains and discomforts which irregular men scatter about them and which in the aggregate so often become formidable obstacles both to happiness and utility; while on the contrary he bestows all the pleasures, and inspires all that ease of mind on those around him or connected with him, with perfect consistency, and (if such a word might be framed) absolute reliability."*

These lines Coleridge was writing in the year 1816, in praise of his friend the poet Robert Southey.

From this initial 'familiar' use, the concept of reliability grew into a pervasive attribute worth of both qualitative and quantitative connotations. In fact, it only takes an internet search of the word 'reliability', e.g. by the popular engine Google, to be overwhelmed by tens of millions of citations (Saleh and Marais, 2006).

From 1816 to 2007 several revolutionizing social, cultural and technological developments have occurred which have aroused the need of a rational framework for the quantitative treatment of the reliability of engineered systems and plants and the establishment of *reliability engineering* as a scientific discipline, starting from the mid 1950's.

The essential *technical* pillar which has supported the rise of reliability engineering as a scientific discipline is the theory of probability and statistics. This theory was initiated to satisfy the enthusiastic urge for answers to gaming and gambling questions by Blaise Pascal and Pierre de Fermat in the 1600s and later expanded into numerous other practical problems by Laplace in the 1800s (Saleh and Marais, 2006; Apostol, 1969).

Yet, the development of reliability engineering into a scientific discipline in itself needed a practical push, which came in the early 1900s with the rise of the concept of mass production for the manufacturing of large quantities of goods from standardized parts (rifle production at the Springfield armory, 1863 and Ford Model T car production, 1913) (Saleh and Marais, 2006).

But actually, the catalyst for the actual emergence of reliability engineering was the vacuum tube, specifically the triode invented by Lee de Forest in 1906, which at the onset of WWII initiated the electronic revolution, enabling a series of applications such as the radio, television, radar and others. The vacuum tube is by many recognized as the active element that allowed the Allies to win the so called 'wizard war'. At the same time, it was also the main cause of equipment failure: tube replacements were required five times as often as all other equipments. After the war, this experience with the vacuum tubes prompted the US Department of Defense (DoD) to initiate a number of studies for looking into these failures.

A similar situation was experienced on the other side of the warfront by the Germans, where chief Engineer Lusser, a programme manager working in Peenemunde on the V1, prompted the systematic analysis of the relations between system failures and components faults.

These and other military-driven efforts eventually led to the rise of the new discipline of reliability engineering in the 1950s, consolidated and synthesized for the first time in the Advisory Group on Reliability of Electronic Equipment (AGREE) report in 1957. The AGREE was jointly established in 1952 between the DoD and the American Electronics Industry, with the mission of (Coppola, 1984):

1) Recommending measures that would result in more reliable equipment;
2) Helping to implement reliability programs in government and civilian agencies;
3) Disseminating a better education on reliability.

Several projects, still military-funded, developed in the 1950s from this first initiative (Coppola, 1984; Raymond Knight, 1991; Denson, 1998). Failure data collection and root cause analyses were launched with the aim of achieving higher reliability in components and devices. These led to the specification of quantitative reliability requirements, marking the beginning of the contractual aspect of reliability. This inevitably brought the problem of being able to estimate and predict the reliability of a component before it was built and tested: this in turn led in 1956 to the publication of a major report on reliability prediction techniques entitled 'Reliability Stress Analysis for Electronic Equipment' (TR-1100) by the Radio Corporation of America (RCA), a major manufacturer of vacuum tubes. The report presented a number of analytical models for estimating failure rates and can be considered the direct predecessor of the influential military standard MH-217 first published in 1961 and still used today to make reliability predictions.

Still from the military side, during the Korean war maintenance costs were found quite significant for some armed systems, thus calling for methods of reliability prediction and optimized strategies of component maintenance and renovation.

In the 1960s, the discipline of reliability engineering proceeded along two tracks:

- Increased specialization in the discipline by sophistication of the techniques, e.g. redundancy modeling, bayesian statistics, markov chains etc. and by the development of the concepts of reliability physics to identify and model the physical causes of failure and of structural reliability to analyze the integrity of buildings, bridges and other constructions.
- Shift of the attention from component reliability to system reliability and availability, to cope with the increased complexity of the engineered systems, like those developed as part of military and space programs like the Mercury, Gemini and Apollo ones.

Three broad areas characterized the development of reliability engineering in the 1970s:

- The potential of system-level reliability analysis (Barlow and Proschan, 1975) motivated the rational treatment of the safety attributes of complex systems such as the nuclear power plants (WASH-1400, 1975).
- The increased reliance on software in many systems led to the growth of focus on software reliability, testing and improvement (Moranda, 1975).
- The lack of interest on reliability programs that managers often showed already at that time, sparked the development of incentives to reward improvement in reliability on top of the usual production-based incentives.

With respect to methods of prediction reliability, no particular advancements were achieved in those years.

In the following years, the last 20-25 years, the scientific and practicing community has witnessed an impressive increase of developments and applications of reliability engineering, aimed at rationally coping with the challenges brought by the growing complexity of the systems and practically taking advantage of the computational power becoming available at reasonable costs. In this respect, the European Safety and Reliability Conferences (www.esrahomepage.org ), to the last edition of which (ESREL 2007) is dedicated the present special issue, have played an important role in providing a forum for fostering these advancements.

The developments and applications of these years have been driven by a shift from the traditional industrial economy, valuing production, to the modern economy centered on service delivery: the fundamental difference is that the former type of economy gives value to the product itself whereas

the latter gives value to the performance of the product in providing the service. The good is not the product itself but its service and the satisfaction of the customer in receiving it.
This change of view has led to an increased attention to service availability as a most important quality and to a consequent push in the development of techniques for its quantification. This entails consideration of the fact that availability is a property which depends on the combination of a number of interrelated processes of component degradation, of failure and repair, of diagnostics and maintenance, which result from the interaction of different systems including not only the hardware but also the software, the human and the organizational and logistic systems.

In this scenario, we arrive at our times. Nowadays, reliability engineering is a well established, multidisciplinary scientific discipline which aims at providing an ensemble of formal methods to investigate the uncertain boundaries between system operation and failure, by addressing the following questions (Cai, 1996; Aven and Jensen, 1999):

- Why systems fail, e,g by using the concepts of reliability physics to discover causes and mechanisms of failure and to identify consequences;
- How to develop reliable systems, e.g by reliability-based design;
- How to measure and test reliability in design, operation and management;
- How to maintain systems reliable, by maintenance, fault diagnosis and prognosis.

# 3 Old problems and new challenges

With reference to the questions posed in the previous Section, old problems afflict reliability engineering. These relate to:

- The representation and modeling of the system;
- The quantification of the system model;
- The representation, propagation and quantification of the uncertainty in system behaviour.

These old problems develop into new challenges when addressed with respect to the modern complex systems and operation tasks.

## 3.1 System complexity

With respect to the complexity of the systems and the modelling of their behaviour, few examples directly relevant to reliability engineering are discussed in the following Sections. Consideration is given to the system as a whole, comprised of its hardware, software, organizational and human elements.

### 3.1.1 Multi-state systems

Modern systems have four basic components: hardware, software, organizational and human. Reliability engineering was originally developed to handle rationally the failures of the components of the first type.

A commonly adopted assumption underlying the quantitative analysis of hardware failures by reliability engineering methods is that systems are made up of binary components (i.e., devices that can be in two states: functioning or faulty). Yet, there are many systems, such as, for example, the manufacturing, production, power generation and gas and oil transportation ones, whose overall performance can settle on different levels (e.g. 100%, 80%, 50% of the nominal capacity), depending on the operative conditions of their constitutive multi-state elements (Figure 1) (Wood, 1985; Garribba et al., 1985; Gandini, 1990; Aven, 1993; Griffith, 1980; Lisnianski and Levitin, 2003; Parikh et al. 2001). In the literature, such systems are referred to as Multi-State Systems (MSS) and their analysis entails the development of new representation, modeling and quantification techniques.

To formalize the analysis of MSS, consider a system made up of $n$ components. Each component $i$ may stay in one of $m_i$ states, $i$=1, 2, …, $n$, so that the system is characterized by a set $S$ of $m_{sys} = \prod_{i=1}^{n} m_i$ states. Concerning the single component, each state is characterized by a different level of component performance. The states of a component $i$ can be numbered according to decreasing performance levels, from state 1 (100%) to state $m_i$ (0%). Let us denote by $w_{i,j}$ the performance of component $i$ when operating in state $j$, $j$= 1, 2, …, $m_i$. Note that a set of performances characterises the single component, independently on the system in which it is embedded. Concerning the whole system, let $W_{\underline{j}}$ denote its performance level when in state $\underline{j} = (j_1, j_2, ..., j_n)$, where $j_i$ represents the state of the $i$-th component, $i$=1,2, ..., $n$. The system performance $W_{\underline{j}}$ is determined on the basis of the individual components' performances, $w_{1,j_1}$, $w_{2,j_2}, \ldots, w_{n,j_n}$ and depends on the system logic of operation of the considered system.

In practice, multi-state systems may be requested to work at different performance levels at different times. For example, the production of electrical and thermal power plants varies according to the daily and seasonal load demands. Assume that at time $t$ a minimum level of system performance $W^*(t)$ is required (Figure 1). The system availability, usually defined in terms of the system being in safe or faulty state, is generalized according to whether its performance is larger or smaller than $W^*$ (for ease of notation, the dependence on $t$ is neglected in the writing). Then, the MSS availability $A(W^*,t)$ of the system at time $t$ is the probability that at that time the system is in any state $\underline{j}$ with performance $W_{\underline{j}} \geq W^*(t)$. If the probability that at time $t$ the system is in state $\underline{j}$ is denoted by $P_{\underline{j}}(t)$, the availability reads:

$$A(W^*,t) = \sum_{W_{\underline{j}} \geq W^*(t)} P_{\underline{j}}(t) \qquad (1)$$

By extension of the definition of the instantaneous availability (1), the concepts of average and limiting availability (Barlow and Proschan, 1975; Aven and Jensen, 1999; Zio, 2007c) may be introduced with reference to the system performance threshold $W^*$, in order to quantify integral, time-independent measures of performance availability of the system (i.e., the probability that the system is in a performance state above threshold for a given percentage of its life time).

A complication of the modeling task comes from the fact that often in practice MSS are such that operational dependencies exist between the system overall state and the state of its components. For example, in a production line with a nodal series structure and no buffers between the nodes (hereafter also called blocks), if one of the nodes throughput changes (e.g. switches from 100% to 50% due to a deterministic or stochastic transition of one of its components), the other nodes must be reconfigured (i.e. their components must deterministically change their states) so as to provide the same throughput (Poszgai and Bertsche, 2003). In the limit, the failure of one of the series nodes implies that the production of the other nodes be turned off. Examples of such systems are those operated according to the so called Just-In-Time production philosophy for reducing manufactory wastes and unnecessary storages by 'producing the right amount at the right time' (Monden, 1998).

When one node is reconfigured, some of its components are changed to new operative states in which they may undergo stress and ageing processes different from those characterizing the states occupied prior to reconfiguration (for instance, in some cases, the components may be considered in a 'no ageing' state while turned off, i.e. in cold stand-by) and this influences the overall availability and performance of the system. Such physical dependencies among the system state and the operation of its components are quite difficult to represent by analytical modeling (Wood, 1985; Garribba et al., 1985; Gandini, 1990; Aven, 1993; Griffith, 1980; Lisnianski and Levitin, 2003), due

to the complexity involved. Yet their modeling has become fundamental in the computation of the realistic production availability of systems such as the oil and gas production plants and others (Zio et al., 2006; Production Assurance ESREL, 2007).

Monte Carlo (MC) simulation (Dubi, 1998; Marseguerra and Zio, 2002) appears to be the only feasible approach to quantitatively capture the realistic aspects of the MSS stochastic behavior (Poszgai and Bertesche, 2003; Zio et al., 2007a). The feasibility of application to realistic cases stems on the capability of properly representing and modeling the multi-state dynamics of the components and systems, e.g. by Petri Nets (Dutuit et al., 1997; Larsen et al., 2000; Schneeweiss, 2004; Sachdeva et al., 2007), and on the possibility of evaluating the model in reasonable computing times, e.g. by biasing techniques (Marseguerra and Zio, 1993 and 2000; Labeau and Zio, 2001). Further developments are certainly needed in this direction, together with some verification on real-size systems.

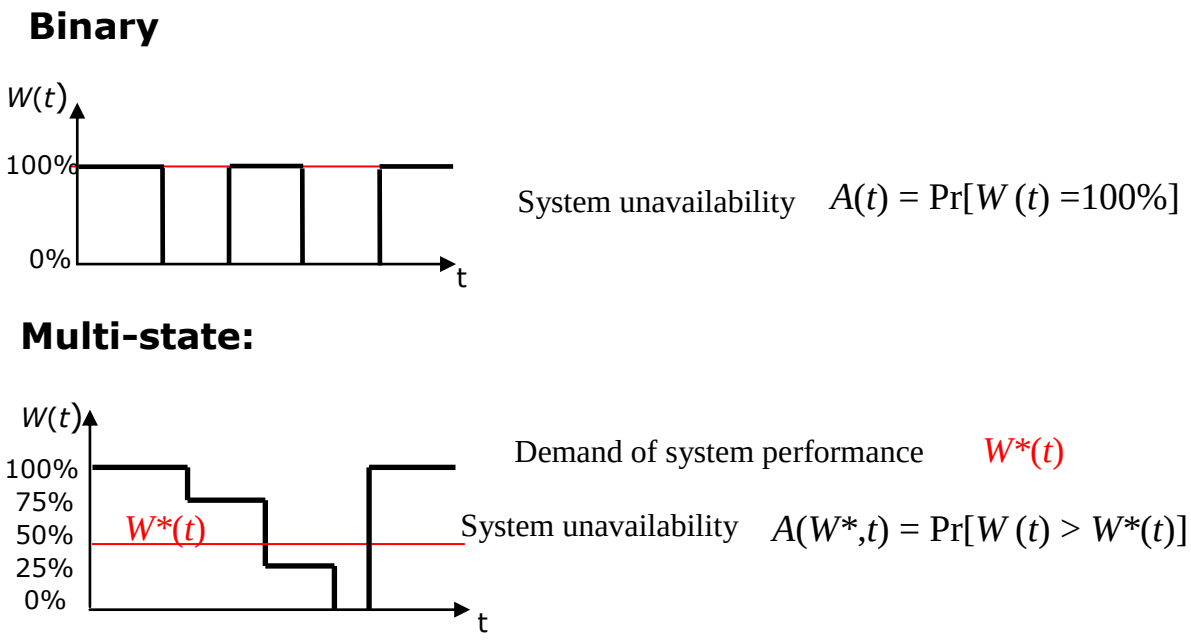



*Figure 1: Binary and multi-state systems*

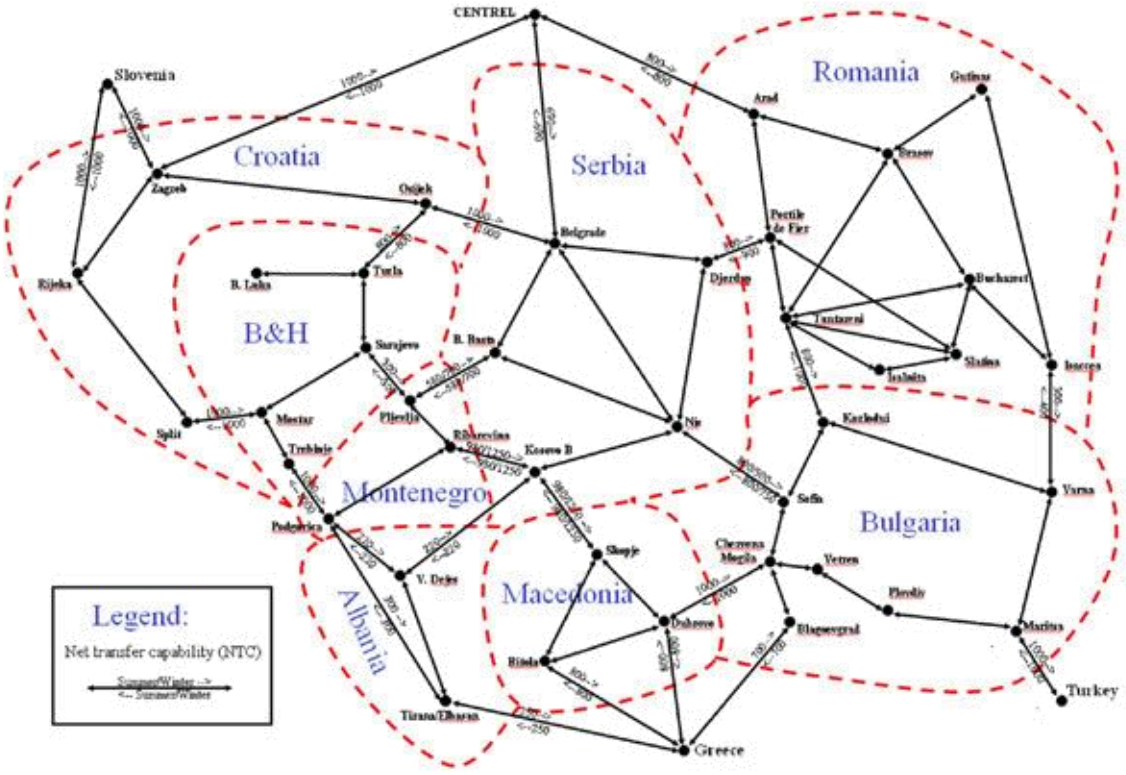
### 3.1.2 Network systems

System reliability methods have been originally tailored to deal with 'fixed', localized systems and plants which can be rationally represented by logical/functional structures of components, albeit

complex. In this representation, the failures of the components are seen with respect to their consequence on the system function.

On the other hand, nowadays many systems of distributed service exist (the so called *infrastructures*, e.g. computer and communication systems, electric power transmission and distribution systems, rail and road transportation systems, water/oil/gas distribution systems), constituted by networks of components (Figure 2). In these systems, there is an additional dimension of complexity related to the difficulty of representing, modeling and quantifying the effects on the system of a failure of a component.

A number of these systems are considered critical for the social welfare of modern societies and thus need priority protection (CNIP, 2006; Birchmeier, 2007). While the EU and other national and transnational administrations are recognizing the importance of this safety issue with specific directives and programs (OHS, 2002; EU 2005 and 2006; IRGC, 2006), it seems that the classical methods of reliability and risk analysis fail to provide the proper instruments of analysis.



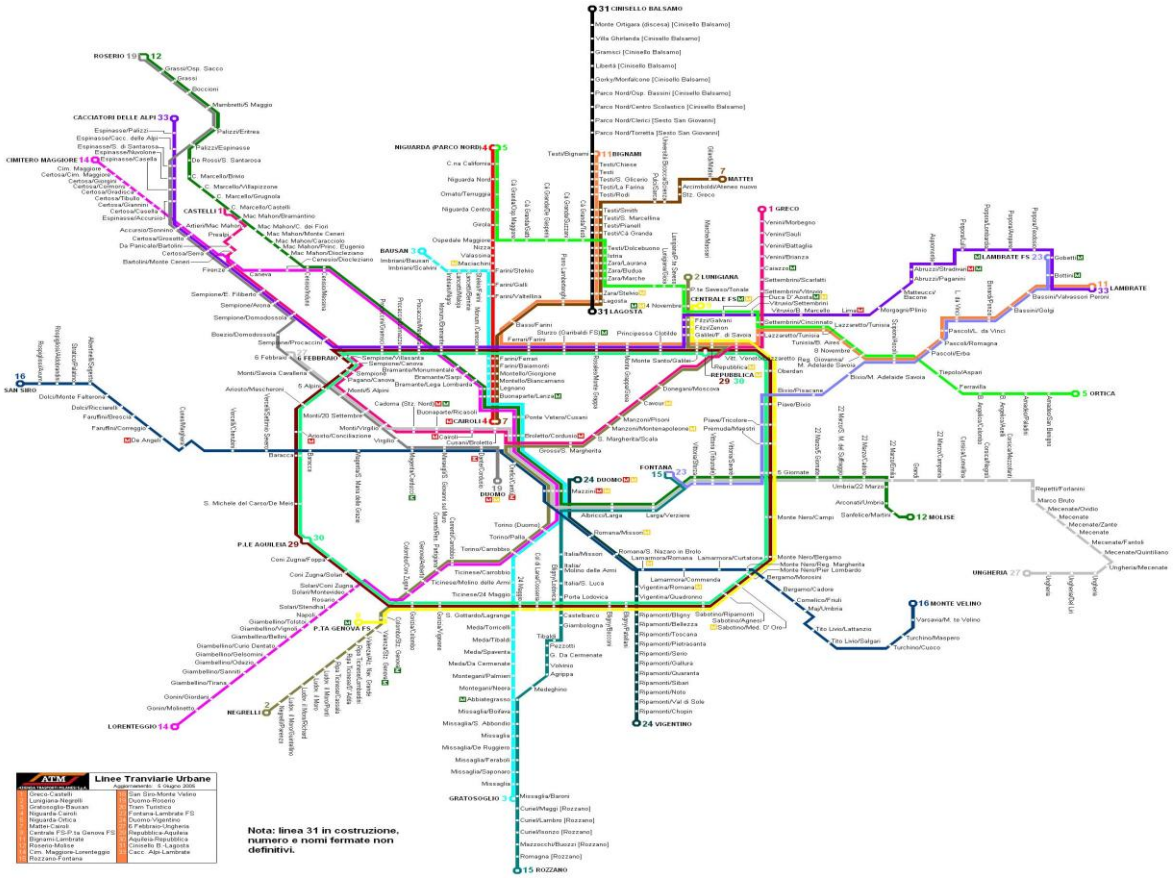



Figure 2: Example of network infrastructures for distributed service: Transnational electrical network (Top) and City Metro Transport System (Bottom)

Indeed, there is an emerging feeling in the community of experts in risk, safety, reliability and security that a new paradigm is needed for analyzing and managing the complex distributed systems and critical infrastructures which constitute the backbone of modern Industry and Society (e.g. computer and communication systems (Aggarwal, 1975; Kubat, 1989; Samad, 1987), power transmission and distribution systems (Jane et al., 1993; Yeh and Revised, 1998), rail and road transportation systems (Aven, 1987), oil /gas systems (Aven, 1987 and 1988) ). Identifying and quantifying the vulnerabilities of such systems is crucial for designing the adequate protections, mitigation and emergency actions against their failures (CNIP, 2006; Rocco et al., 2007; Vulnerability ESREL, 2007). These needs are enhanced in a World where deregulation of the services is favored and malevolent acts of terrorism and sabotage are a serious threat (CNIP, 2006; Rocco et al., 2007; Vulnerability ESREL, 2007).

The current methodologies of reliability engineering, risk assessment and management are applied successfully on man-machine-environment systems with well-defined rigid boundaries, with single, well-specified targets of the hazard and for which historical or actuarial data (e.g. accident initiators

and components failure rates and empirical data on accident consequences) exist in support to robust quantification models which account for the uncertainties deriving from both random variations in the behavior of the elements of the system under analysis and from lack of knowledge of the system itself (Apostolakis and Lemon, 2005).

In the current framework, reliability engineering aims at searching for the causal links among the system elements (components, structures, people, etc.) and modeling and integrating their behavior so as to quantify that of the system as a whole.

On the other hand, risk management aims at achieving rational, risk-informed decisions by carrying out an optimization process aimed at maximizing specified preferential objectives in presence of uncertainty. The simplest example of such process is the classical cost-benefit analysis.

This approach to reliability engineering and risk analysis (assessment and management) of complicated technological systems (Kastenberg, 2005):

- assumes that the system has fixed boundaries, there is a fixed well-defined target and there are actuarial data available to support the quantification models,
- is sustained by the classical Newtonian/Cartesian view of the World, which is founded on the following creeds on the system behavior:
    1. it can be understood from the behavior of its constitutive elements (reductionism) and their causal links (cause-and-effect);
    2. it can be determined from objective empirical observations (subject/object dualism).

As illustrated in (Kastenberg, 2005), the above framework of analysis may not be fully apt to deal with many existing complex network systems which, on the contrary, are characterized by a behavior which:

- emerges as a whole and hence cannot be understood and properly described by looking at its constitutive parts, which do not exhibit such behavior when taken by themselves (emergent/holistic property),
- may change significantly for small changes in the input (chaotic),
- can partly be described only subjectively (subjective).

The above characteristics of the newly arising complex network systems are such that societal and environmental impacts of accidents and attacks are no longer geographically local (e.g. a blackout in a power transmission and distribution network or a malevolent attack to a transportation network) nor clearly perceptible in time because either spreading very quickly (a virus in the Internet) or very slowly (an accident in a radioactive waste deposit whose consequences may affect future generations).

The new risk scenario of modern Industry and Society briefly depicted above creates some unprecedented challenges to research and practice, such that a new paradigm of risk may be in order and new methods for reliability and risk analysis needed.

In particular, an innovative and promising approach to the analysis of complex technological network systems and infrastructures comes from the findings of Complexity Science (Kauffman, 1993; Capra, 1996; Science, 1999; Bar-Yam, 1997; Barabasi, 2002). Recent advances in this field indicate that many complex systems, technological, natural and even social, are hierarchies of networks of components (also called nodes, vertices or elements) interacting through links (also called edges, arcs or connections). Although the properties of the individual components can usually be characterized in laboratory, these isolated measurements bring relatively little information on the behavior of the large scale interconnected systems in which they are embedded. This is due to the fact that it is from the local interaction of the components in the interconnected network that the system behavior emerges as a whole.

The apparent ubiquity of networks leads to a fascinating set of problems common to biological, ecological, technological and social complex systems, regarding how the underlying network topology influences the system behavior and its characteristics of stability and robustness to faults and attacks. For example, the topology of the power grid affects the robustness and stability of power transmission (Carreras et al, 2002; Crucitti et al, 2004; CNIP, 2006; Jonsson et al. 2007; Rosato et al., 2007).

In this view, the actual structure of the network of interconnections among the components is a critical feature of the system: the stability and robustness of these systems depend on the redundant wiring of the functional web interconnecting the system's components; yet, error tolerance and attack robustness are not shared by all redundant networks (Albert et al., 2000).

For these analyses to be of use at the decision making level, efforts must be made to bring into the picture the characteristic safety and reliability attributes of the network components to analyze the properties that emerge at the system level (Zio, 2007a). The indicators thereby developed can be exploited for the analysis of the vulnerabilities of network systems and thus for their optimal design, operation and management.

The above analyses must be corroborated by detailed system modeling of a limited set of design and accident scenarios, e.g. by agent-based and Monte Carlo simulation (CNIP, 2006).

Furthermore, dependences need to be adequately modeled to investigate the interactions among complex infrastructure systems, leading to the so called *systems of systems* (Carreras et al., 2002; CNIP, 2006; Bologna, 2007). The European electric power supply system serves as a good illustrating example, facing greater and tighter integration, also of new intermittent power sources,

following the liberalization of most markets and being closely interconnected with other infrastructures, particularly the information and communication network. More in general, communication, power, transportation networks are complex infrastructure systems which interact with each other in even more complex ways: from these interactions increased risks of failures may arise in the individual systems from unexpected emergent behavior. Investigating the risks and vulnerabilities for these kinds of systems has to go beyond the usual cause/agent-consequence analysis to be able to focus on spill-over clusters of failures in case of strong interdependencies (Eusgeld and Kroger, 2008).

To investigate these issues, new approaches and paradigms of dependence analysis need to be formulated. Indeed, in practice there seems to be no single 'silver bullet solution' to the problem of analyzing the risks associated to interdependent critical infrastructures. Rather, in view of the limitations and deficits of the available methods, albeit mature, and of the need of restricting the computation times for application feasibility, a framework of analysis seems in order to effectively integrate the different methods in a problem-driven approach to solution. Such framework may incorporate elements of Complexity Science methods of network analysis for the initial screening of the vulnerabilities of a critical infrastructure, PRA methods of quantitative scenario analysis (Haarla et al., 2008; Koonce et al., 2007; Bier et al., 2006; Michaud et al., 2006; Patterson et al., 2006; Salmeron et al., 2004) and agent-based modeling to further deepen the vulnerability assessment of the screened scenarios (Schlapfer et al., 2008).

### 3.1.3 Organizational and Human Reliability Analysis

As previously stated, reliability and safety are system properties which emerge from the interactions of all the diverse system constituents, hardware, software, organizational and human. Indeed, the experience accumulated on occurred industrial accidents in the last few decades has clearly shown that the organizational and human factors play a significant role in the risk of system failures and accidents, throughout the life cycle of a system. This is due also to the fact that the reliability of the hardware components utilized in technological systems has significantly improved in recent years, particularly in those systems requiring high safety standards like those employed in the nuclear and aerospace applications. As a consequence, the relative importance of the errors of the organizations managing the systems and of the human operators running them on the risks associated to the operation of these systems has significantly increased. This explains the significant focus on Organizational and Human Reliability Analysis (HRA) and on its full integration within systematic

risk analysis and reliability assessment procedures (Gregoriades et al., 2003; Duval et al., 2007). This widens the scope of the analysis to the so called 'socio-technical' systems, considering that human and technical performance is influenced by the organization and management of the industrial activities, by the safety culture of the organization and by other exogenous factors such as regulations, market pressures, political pressures etc. (Trbojevic et al., 2007).

Even more, insights from research on failures in complex systems have revealed that safety is an emergent property of a system and their constitutive elements, rather than a resultant one. In this view, systems should not only be made reliable, i.e. with acceptably low failure probability, but also *resilient*, i.e. with the ability to recover from disruptions of the nominal operating conditions (Hollnagel et al., 2006). In this regard, a new field of research in *resilience engineering* is emerging, for understanding the factors that determine human and organizational performance and for duly incorporating the related risks into the system analysis and management tools, throughout the life cycle of the system and accounting for the short- and long-term effects on risk of organizational and management decisions and design and operation changes.

Compared to technical components, the human and organisational components of a technological system are characterized by their multidimensional aspect and intrinsic complexity due to the many nonlinear interactions which influence their behaviour. Any attempt to capture these aspects into a model must face the difficulties related to the subtlety of the scarce information at disposal and its subjective interpretation (Duval et al., 2007).

Yet, a number of qualitative and quantitative methods have been proposed for incorporating organisational factors in risk assessment, aiming at the explicit modelling of the influence of management and organisational factors to be properly evaluated (Hurst et al., 1991; Wreathall et al., 1992; Murphy and Pate-Cornell, 1996; Oh et al., 1998; Reason, 1998; Oien, 2001; Aven et al., 2006).

However, although the role of human and organizational factors in accident causation is well recognized (Rankin and Krichbaum, 1998; Flin, 2007), at present most industries still do not have formal methods for the quantification of their effects on risk. Human and organizational errors are still mainly controlled through traditional quality assurance and quality control measures. This approach may be adequate for simpler systems and operations but are clearly not sufficient for managing major hazards in complex operations such as a process plant or nuclear power station.

For this reason, industries such as the nuclear, oil & gas, maritime have been researching the field, particularly with the aim of providing quantitative methods for evaluating organizational and human error probabilities and their effects. To achieve the objective, a framework for the proper representation and modeling of socio-technical systems is needed (Gregoriades et al., 2003; Duval

et al., 2007). This may be achieved by the effective combination of qualitative and quantitative representation and modeling methods, e.g. the 'Qualitative and Quantitative Bayesian Belief Networks' (QQBNs) (Mosleh, 2007) and influence diagrams (Vinnem, 2007).

With respect to modeling human errors, the early methods of analyses, the so-called 'first generation' ones like the Technique for Human Error Rate Prediction (THERP) (Swain and Guttman, 1983), Accident Sequence Evaluation Program (ASEP) (Swain, 1987) and Human Cognition Reliability (HCR) (Hannaman et al., 1984 and 1985), are built around the pivotal concept of human error: because of the inherent deficiencies of humans, they naturally fail to perform tasks just like mechanical, electrical, structural components do. In this view, it makes sense to assign a probability of failure of a human operator in performing a task of given characteristics. Thus, the quantity Human Error Probability (HEP) can be defined with respect to a given task and appropriately modified in consideration of the environmental conditions under which it is performed. The factors representing the effects of the environment on the human performance of a task are called Performance Shaping Factors (PSFs) or Performance Influencing Factors (PIFs). The point of view of 'first generation' methods with respect to failure of a human performing a given task is thus clear: the task characteristics, captured quantitatively in the HEP assignment, are regarded as the most influential factors for the estimation of the probability of human failure, whereas the environment in which the task is performed, which is represented by the PSFs and PIFs, is considered as a minor, corrective factor.

On the other hand, experimental results from extensive studies of human performance in accidents have shown that the importance of the contextual conditions in which the task is performed is greater than the characteristics of the task itself. This has led to a change in the focus of human failure analysis: if the context is the major factor affecting human performance failure, the relation between the context and the probability of human failure should be modeled. This is the underlying principle of the so-called 'second generation' methods of HRA like the Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel., 1998) and A Technique for Human Error Analysis (ATHEANA) (Cooper et al., 1994).

Many of the methods above mentioned have proven useful in various situations and yet the community of experts in the field seems to agree that further understanding and development in this complex issue are needed as a proper understanding of organizational and human errors, and their causation, helps in establishing effective safety management systems to control and minimize also these errors, thereby improving safety.

To this aim, simulation is recognized to provide significant potential understanding into the dynamics of human performance (Boring, 2007). The logs produced by simulation runs can be

analyzed by experts and used to inform an estimate of the likelihood of human error. For this to be successful, controlled expert elicitation procedures must be set up to avoid biases in the estimation procedure. Otherwise, the simulation results can provide information useful for the estimation of the PSFs which can eventually be quantified to produce HEP values (Boring, 2007). This requires establishing a mapping between measures of performance from the simulation and the PSFs (Boring, 2006). Finally, it is also conceivable to set specific criteria of successful performance in given tasks (e.g. time to complete the task) by which the virtual performers are evaluated (Bye et al., 2006): by counting the number of times that the task is not successfully performed by the virtual performers, one may compute a frequency of failure to be used as estimate of HEP (Boring, 2007).

In this view, an investigative effort worth of mention is the EU-funded project Virtual Reality and Human Factors Applications for Improving Safety (Virthualis, http://www.virthualis.org/ ), aimed at developing a system and technological platform that tackles safety by adopting Virtual Reality (VR) technology to explore how human factors influence safety issues. VR is expected to enable industry to make experiments in a safe and economic way, in a virtual environment rather than in the real plant where such experiments cannot be performed because of the costs and risks involved. Such experiments can provide the needed measurements and qualitative evaluations of human factors and serve as testbeds of different hypothesis, scenarios and methods for reviewing the human organisation and work processes, improving design quality for better safety in new or existing plants and retrospectively examining past accidents to gain hints for the future procedures.

Finally, in practice the choice of which HRA method to use for a particular safety assessment will remain a difficult problem. This calls for procedures of comparison and validation in order to guide the choice of the adequate approach for a given situation.

As mentioned above, in order to perform a comparison of the available HRA methods the best approach is virtual simulation. In this regards, a pilot study is being undertaken at the Halden Man-Machine Laboratory's (HAMMLAB) facility of the OECD Halden Reactor Project (HRP) with the aim of providing the technical basis for the comparison of the performance and findings of different HRA methods. The study is intended to be a pilot test aimed at establishing a first guidance in the assessment and improvement of HRA methods through the information gained by simulator data. The initial testing study will focus on the performance of a number of crews in the Hammlab experimental facility, which reproduces the digital instrumentation and control systems and equipments in actual nuclear Pressurized and Boiling Water Reactors (PWRs and BWRs). The comparison between the results of the HRA methods and the actual experimental performance is to be made in terms of the "driving factors" that most influence the human performance and of the estimated values of Human Error Probability (HEP).

In principle, the use of human operators in virtual simulators allows capturing the full spectrum of human PSFs for a given task. However, the possibility of repeated trials is limited and the need of forcing error-likely situations may affect the scenario realism.

Also, although the bulk of the simulation analyses focuses on the qualitative modeling of crew behavior, the quantitative results play a fundamental role, as they eventually need to be input into the reliability and risk analyses. In this respect, the experiments are expected not to yield statistically significant experimental values of HEPs, due to the very high level of performance of the trained crews and the small number of simulated sessions; henceforth a surrogate model for retrieving experimental values of HEPs is needed. The quantitative evaluation of the results of these simulations in terms of crew performance and human error probabilities is expected to be quite a difficult task and new methods will need to be developed to address the issue (Zio et al., 2007b).

Concurrent with the emergence of simulation modeling of the dynamics of human performance, a number of new HRA methods are being developed to adequately account for the dynamic progression of human behaviour leading up to and following human failure events (Mosleh and Chang, 2003; Reer et al., 2004; Strater, 2005; Boring, 2006; Trucco et al., 2006). These are possible thanks to the increase of computer power available and aim at augmenting first and second generation methods by the use of virtual environments for mimicking the performance of humans in actual scenarios, thus providing a dynamic basis for HRA modeling and quantification. In these simulation-based HRA methods, a dynamic model is implemented to reproduce human decisions and actions during the scenario development and uses the results as basis for human performance estimation. A variety of human behaviours may be modeled across a series of Monte Carlo replicas to arrive at a frequentist estimation of HEPs. Of course, the modeling tasks associated to the simulation pose significant challenges in the need for accounting of the scenario dynamics, inclusive of the eventual dependency among successive events (Zio et al., 2007c). Dependency is typically accounted for by modifying the probability of downstream errors without systematically modeling the progression of the PSF levels across the successive events. On the contrary, a dynamic simulation allows accounting for the evolution of the PSF levels and of their effect on the outcomes of the downstream events (Boring, 2007). This brings up the issue of scenario granularity regarding which level the events in the scenario can be decomposed to. Care must be taken to ensure that the level of task decomposition be compatible with the HRA approach being adopted.

As a final remark on the methods, while first and second generation methods will continue to be applied when needed and the latter will continue to be improved, there are exciting developments in HRA on the horizon of human performance dynamic simulation.

### 3.1.4 Software for safety and reliability for software

When considering the requirements on the safety integrity levels of modern safety instrumented systems and components, their characteristics of reliability, availability, functionality and safety become parts of a unitary view of the safety and control functions involved. Several international standards give requirements and guidance on how to design, operate and maintain such systems (Hokstad and Corneliussen, 2004). In analyzing these systems, the characteristics of the implemented software and hardware protective barriers must be considered. Although hardware barriers are considered 'more reliable/available' than software barriers, due to the longer experience in their performance, this often overlooks the extensive work (often manual) involved in proof-checking the proper functioning of hardware barriers. Indeed, the chosen test interval is for this reason substantially longer than that for software barriers, which are easily integrated in automatic self-test procedures, with consequent very low probabilities of failures on demands (PFDs) and mean fractional dead times (MFDTs). Practical examples show that MFDTs for comparable tasks differ by a factor of more than 100 in favor of software barriers (Frankhauser, 2001). On the other hand, in complex systems even daily self-tests are not able to reveal all potential failures which might limit the proper functioning of the provided barriers. Therefore, proof-checks performed at regular intervals are still required to cope with *undetected dangerous* hardware failures, which are not detected by automatic self-tests whose diagnostic coverage is never complete (probability of detecting a dangerous failure less than one).

From the modeling point of view, the complementation of hardware and software barriers for system functionality and safety challenges the reliability analysis models which must give due account not only to the processes of failure occurrence and repair completion but also to the performance of self- and proof-checking tests.

On the other hand, software reliability is an important challenge in itself for all industries which employ digital Instrumentation and Control (I&C) devices, mostly of the COTS type (Commercial-Off-The-Shelf). When developing models and methods for the analysis of software failure behavior, perhaps the most disturbing thing is that the concept of failure mode is not the usual one for hardware components. Indeed, whereas analog systems are physical, digital systems do not follow physical laws of degradation or failure given that the input determines the output being right or wrong (Software Reliability ESREL, 2007).

In general, two points of view can be taken on software failures (Apostolakis, 2006b): a software-centric approach which looks for the definition of failure modes and the evaluation of their probabilities, just like in any reliability approach of hardware components; a system-centric viewpoint which is funded on the practical observation that most failures in software occur due to

specification and requirement errors, i.e. software design errors which are quite different from the physical failure characteristic of the hardware components.

An approach to the quantitative analysis of software failures is by fault injection methods which deliberately inject faults in the software and count the number of times that the software maintains its function in spite of the injected fault (Voas, 1997; Gran and Thunem, 1998; Hiller et al., 2001 and 2002; Abdelmoez et al., 2004). Given the many processing paths of software and the corresponding potentially hidden failure modes, the method remains controversial and needs extensive runs for building high confidence in support of the results. Furthermore, case studies must be specifically tailored to test susceptibility to common mode failures and verify whether fault injection is an adequate method to address such problem.

Hence, a more feasible approach to software reliability that is followed in practice is one which aims at a systematic control of the software development process for building fault tolerance and confidence in its reliability. The objective is to evaluate different fault tolerant approaches throughout the software process development. This entails the capability of anticipating latent errors and providing for their remedy. By preventing errors from progressing into failures that threaten system safety, these fault tolerant mechanisms often play a crucial role in ensuring the qualification of a digital instrumentation and control system (Fredriksen and Winther, 2007). In this sense, fault tolerance complements fault avoidance.

In any case, assessing software failure probabilities requires a standard process for collecting, analyzing and using digital system data from different applications, accounting for their peculiarities (e.g. in nuclear plants, digital systems will mainly be used for actuating safety systems and not for controlling and running the plant as in the process industry) and taking into consideration the rapid changes in the technology (with time constant of few months in certain cases). For example, a major automotive supplier is developing a new database which makes it possible to detect most failures occurring during usage, including software failure (Braasch et al., 2007).

Furthermore, time-dependence of the system behavior cannot be neglected when digital I&C are part of the system; on the other hand, the reliability analysis methods currently used in practice account for the time variable at most by discretization in a sequence of macroscopic events (NUREG/CR-6901, 2006). The challenge is then twofold: on one side, to develop procedures and methods of inclusion in the current analysis methods of dynamic reliability models with digital systems, e.g. expanding in a system fault tree the event related to I&C failure; on the other side, to continue the efforts of developments of methods of integration of dynamics and reliability analysis, both through advancements in the conceptual and analytical modeling (Aldemir et al., 1994;

Alzbutas et al., 2007) and implementations in simulation tools for practical applications (NUREG/CR-6901, 2006; Mosleh, 2007).

## 3.2 Complex system operation tasks

Complex tasks need to be performed on modern systems in order to ensure their reliability throughout the life cycle. These tasks need to be properly represented, modelled, analyzed and optimized.

### 3.2.1 Maintenance

One task which has gained significant relevance is *maintenance*, for its important fallbacks to both productivity and safety (SAFERELNET, 2006a; ESReDa, 2007; Maintenance ESREL, 2007).

Modern engineering systems are ideally designed for profitable operation throughout their service life in compliance with given requirements and acceptance criteria typically related to the safety of the personnel and the risk posed to the public and the environment. For ensuring this, it is necessary to control the development of deterioration processes by appropriate planning and performing of inspections and maintenance actions. Decisions must be taken with respect to what, how and how often to inspect and maintain. These decisions need to be made so as to minimizing the impact on the productive and safe operation of the system. In other words, inspections and maintenances must be planned so that a balance is achieved between the expected benefits and the corresponding expected potential consequences.

From the point of view of the production company, the primary objective of any task and operation on its systems and components is to maximize production profit and minimize all losses, including assets ones. Obviously, occupational and public safety, environmental and other requirements must be satisfied as enforced by regulations. To this aim, maintenance must ensure that the systems and components reliability and availability characteristics be kept consistent with the long- and short-term requirements of the planned production and regulatory directives, at a minimum resource cost.

The goal of effective maintenance planning is then minimizing unplanned downtime. In practice, taking into consideration the financial aspects of system operation, the maintenance philosophy of a production plant basically boils down to performing the optimal maintenance plan that is consistent with the optimization of production and plant availability, while not compromising safety and the associated regulatory requirements.

The formalization of the above into a modeling approach to identifying the optimal maintenance strategy for the components of a production system must consider the production goals, the safety,

health and environment objectives, the maintenance costs and penalties for lost production. This needs to be done while accounting for all the interacting elements of system operation and the many sources of uncertainties which affect them in the integrated process of system life.

In practice, the solution to this complex multi-objective optimization problem stands on: 1) the proper representation of the dynamic interactions among the different system elements which affect the system behavior and its maintenance (e.g. by Petri Nets or BBNs; Zille et al., 2007), 2) the proper reliability, maintenance, production and economic modeling of the involved processes (e.g. by Petri Nets and Monte Carlo simulation; Châtelet et al., 2002), 3) an efficient engine for the search of the potentially optimal strategies (e.g. by the arising evolutionary computational methods such as genetic algorithms; Marseguerra and Zio, 2000; Marseguerra et al., 2006; Genetic Algorithms ESREL, 2007) and 3) a solid decision making-theory structure for their evaluation (SAFERELNET, 2006a).

An effective, pragmatic way to proceed for establishing maintenance programs in practice has been shown to be the *Reliability Centered Maintenance (RCM)* approach (Nowlan and Heap, 1978; Rausand, 1998). This method directs maintenance efforts towards those parts and units which are critical from the point of view of reliability, safety and production regularity. The critical components are identified by means of properly defined importance measures. A decisional logic is supported by specific forms to identify the worthwhile maintenance activities and their timing. The approach is more qualitative than the mathematical models for maintenance optimization but it is more all-embracing than these models which have only a limited capability of capturing all aspects involved in system maintenance because of the need of introducing simplifying assumptions for their solution (Horton, 1992).

Benefits from the introduction of quantitative decision tools within RCM are continuously sought to integrate all the above mentioned maintenance-relevant elements within an effective reliability-based and risk-based Maintenance Management System employing decision theory for minimizing overall service life costs including direct and implied costs of failures, repairs, inspections and maintenances. These systems are seeking the maturity of practical procedures and indeed start to be applied in various industries from the early development stages of any new product, process or system (Jovanovic, 2003)

Maintenance Management Systems allow the efficient management of the flow of materials, the co-ordination of the internal activities with the ones of the suppliers and the proper dialogue with the productive sector to time the activities in harmony with the necessities of equipment availability for production. Indeed, forecasting of production demand is a key element to integrated production and maintenance planning and control. This requires the complicated handling and processing of a great

volume of data in reasonable time which can be achieved only with the support of an efficient computerized system of data processing.

From the above, it appears that modelling and optimization is the technical support for proper maintenance planning and practice. Yet, in spite of the many efforts of many researchers in the field it seems fair to say that in some industries the situation is not brilliant and that a significant gap still exists between theory and practice. Indeed, maintenance programs are in many cases still based on the vendor's recommended maintenance schedules which are usually conservative. More efforts in the direction of closing the gap should be strongly advocated. From the model developers side, care should be put in avoiding the over-parameterization of the models which often are too detailed and need the estimation of too many parameters for their application in practice to be feasible (van Rijn, 2007); from the industrial users point of view, a more open-minded attitude should be undertaken with respect to investments and endeavours in the development of protocols for maintenance data collection and analysis, so as to provide the information necessary to build properly calibrated and tailored maintenance models.

Paradoxically, plant owners and system managers are constantly looking for opportunities for reducing maintenance costs and improving productivity, while not compromising safety. On one side, these opportunities may come from optimized preventive dynamic maintenance schemes based on the estimation of the rate of occurrence of failures (ROCOF) during the system lifetime. Indeed, this index allows tracking the system reliability growth or decrease and can thus play a fundamental role in determining the optimal timing of maintenance interventions and replacements (Ascher and Fengold, 1984). In this regard, the challenge is to be able to compute the ROCOF under realistic assumptions of system dynamic evolution (Yeh, 1995).

An alternative, complementary opportunity which is receiving increased attention is that of condition-based maintenance strategies founded on the concepts of monitoring, fault diagnostics and prognostics (Figure 3) (Jarrell et al., 2004; Korbicz et al., 2004). As in Medicine, a clinical picture and diagnosis can be made with the values of some measured parameters related to the health condition of a human being, in any kind of equipment it is also possible to have an idea about its functional condition from the knowledge of the evolution of its significant parameters.

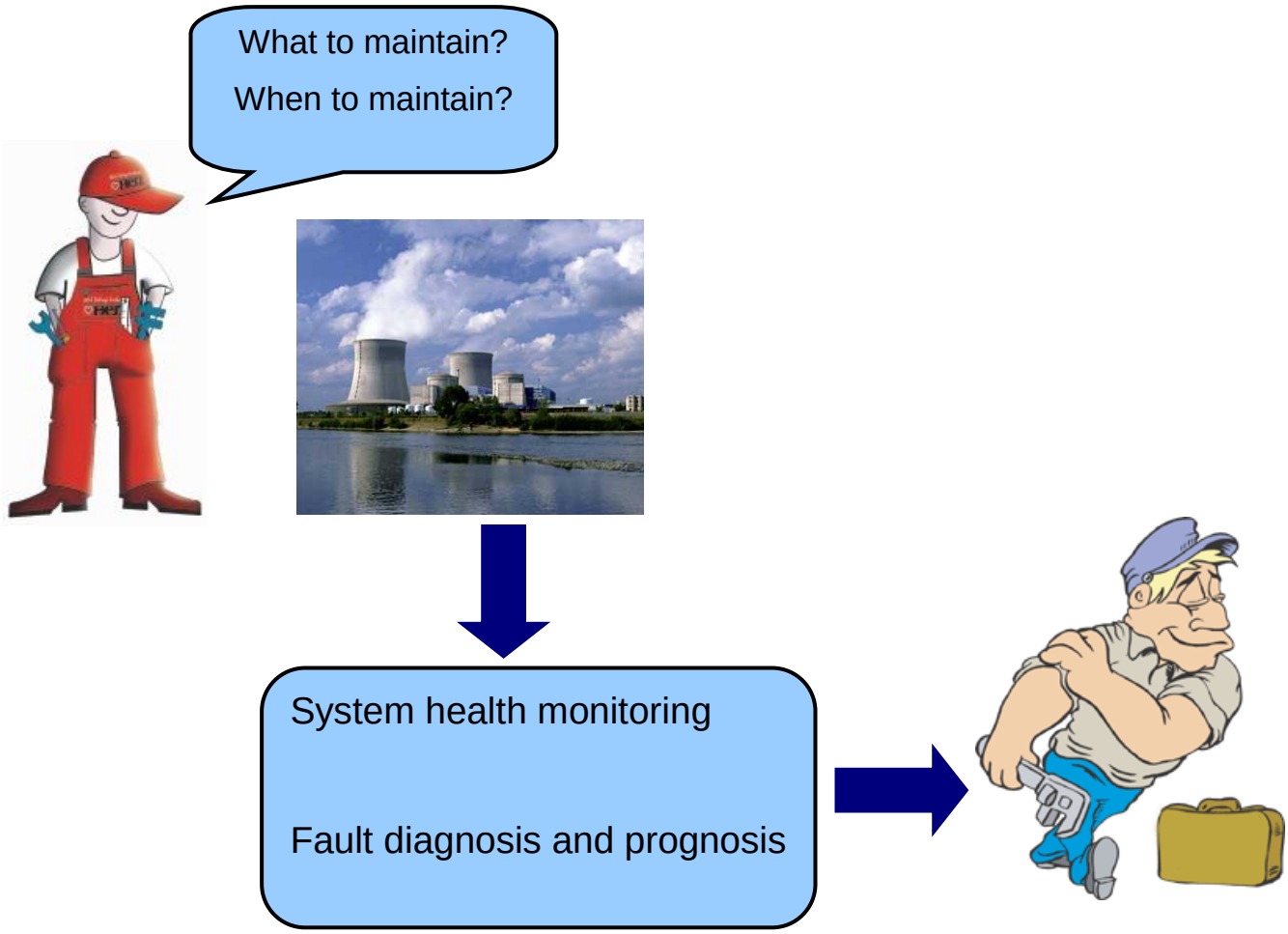



Figure 3: Monitoring, fault diagnosis and prognosis for maintenance

To this aim, equipment and components are inspected periodically by manual or automatic systems to monitor their condition and to identify their level of degradation. A decision is then taken regarding replacement or maintenance, and this is based upon an analysis of the monitored data (Figure 4).

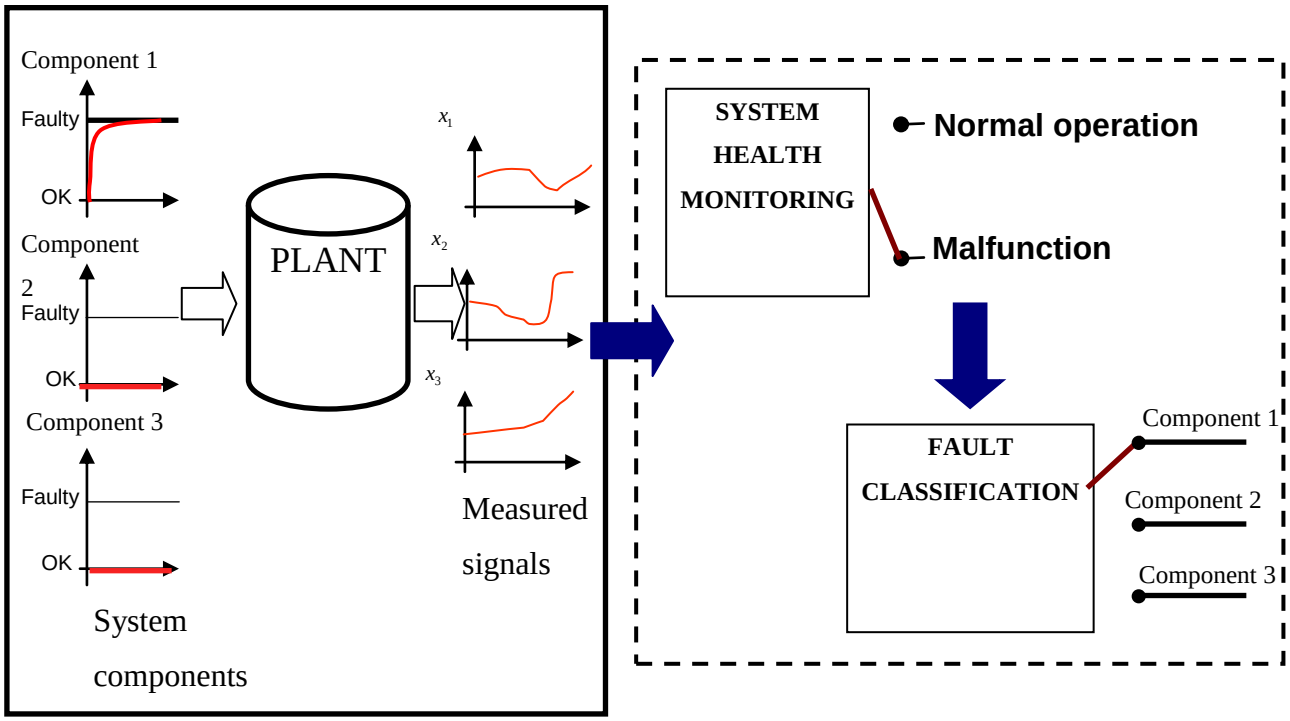



Figure 4: System health monitoring

In this view maintenance is carried out when a measurable machine condition shows the need for repair or replacement. This strategy aims at identifying problems in equipment at the early stage so that necessary downtime can be scheduled for the most convenient and inexpensive time. This allows a machine to run as long as it is healthy: equipment is only repaired or replaced when needed as opposed to routine disassembly. By so doing, one aims at achieving maximum availability, minimizing unscheduled shutdowns of production, scheduling maintenance actions as economically as possible.

Usually, the condition of the system concerned is monitored at a regular interval and once the reading of the monitored signal exceeds a threshold level a warning is triggered and maintenance actions may be planned. Obviously, the monitoring interval influences the operating cost and overall performance of the plant: a shorter interval may increase the cost of monitoring, whereas a longer one increases the risk of failure.

On the other hand, condition monitoring should be reliable in order to avoid false alarms. A decision must be taken every time an alarm is indicated. To ignore an alarm may give rise to serious consequences. The first option is to make further investigation of the alarm, without stopping the machine; the second option is to stop the machine for an overhaul of the suspected part. In the first option, a false alarm would result in extra cost due to the time and manpower necessary to make the

diagnosis. The second option could result in greater losses, where lost production and manpower costs occur simultaneously. The greatest losses will occur when ignoring the alarm.

Finally, condition-based maintenance implies that maintenance activities be scheduled in a dynamic way, since the execution times of certain activities will be continually updated as condition information becomes available. Such scheduling is significantly more difficult than scheduling the static policies implied by routine preventive maintenance.

Indeed, the dynamic scheduling of condition-based maintenance represents a challenging task which requires the integrated simulation of the system state transitions and the prediction of the monitored physical variables which represent the evolving components condition. Hence, it is important to develop reliable models of components degradation and for the estimation and prediction of its evolution. Given the complexity of the processes underlying mechanical and structural degradation and the ambiguous and uncertain character of the experimental data available, one may have to resort to empirical models based on collected evidence, some of which may very well be of qualitative, linguistic nature. In this direction, soft computing techniques, such as neural networks and fuzzy logic systems (inferential systems based on the mathematics of fuzzy sets), represent powerful tools for their capability of representing highly non-linear relations, of self-learning from data and of handling qualitative information (Zio, 2007b). Embedding these models within the simulation of the stochastic processes governing the system life could represent a significant step forward for the evaluation of the safety and reliability of a system under condition-based maintenance and, thus, for the definition of the optimal thresholds of the monitored variables which determine the dynamic scheduling of maintenance intervention.

A condition monitoring system will be efficient only if the information retrieved from the monitoring equipment is relevant and it is filed, processed and used by the management in a timely manner, so that the decisions can have effectiveness and result in an increase of productivity (Roverso et al., 2007). The capability of acquisition and handling of system and process information in real time (Figure 5) is therefore a necessary condition for performing on condition maintenance to optimize the performance of the machines and to maximize their use and productivity.

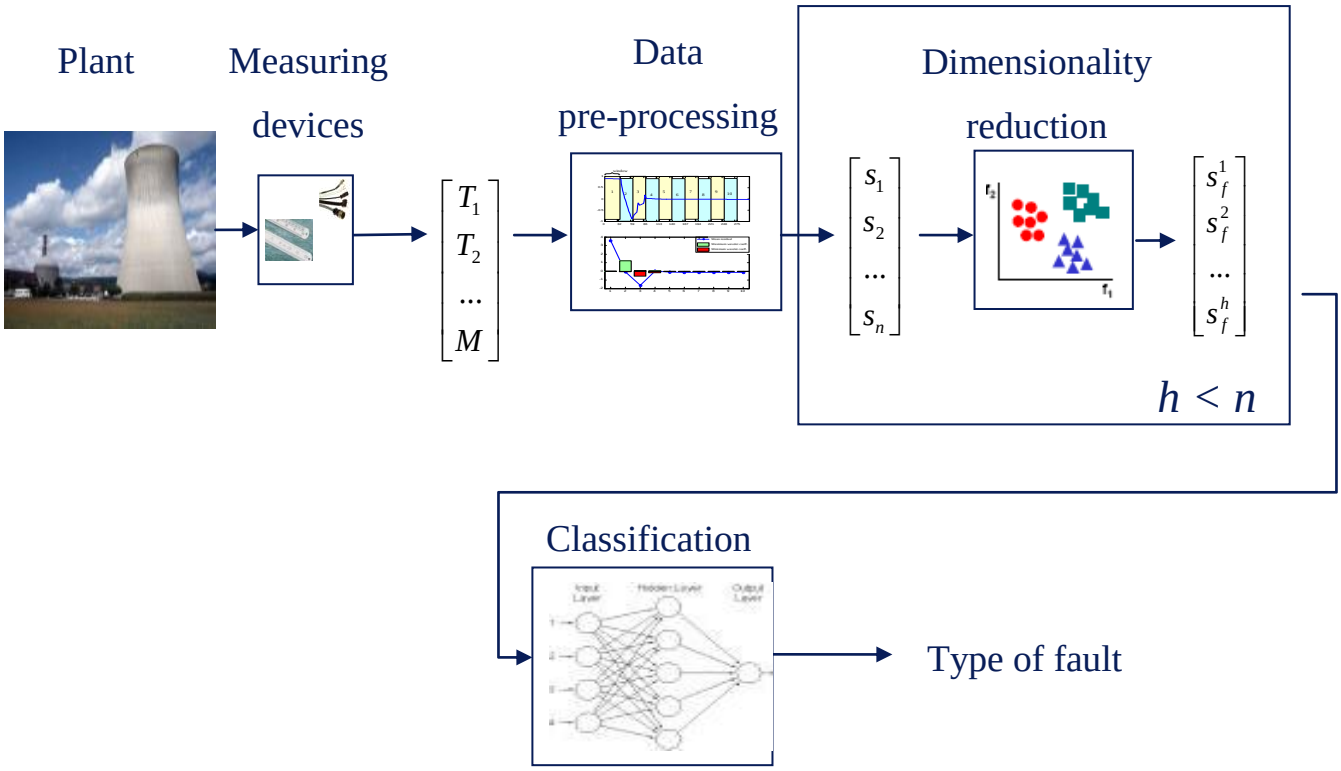


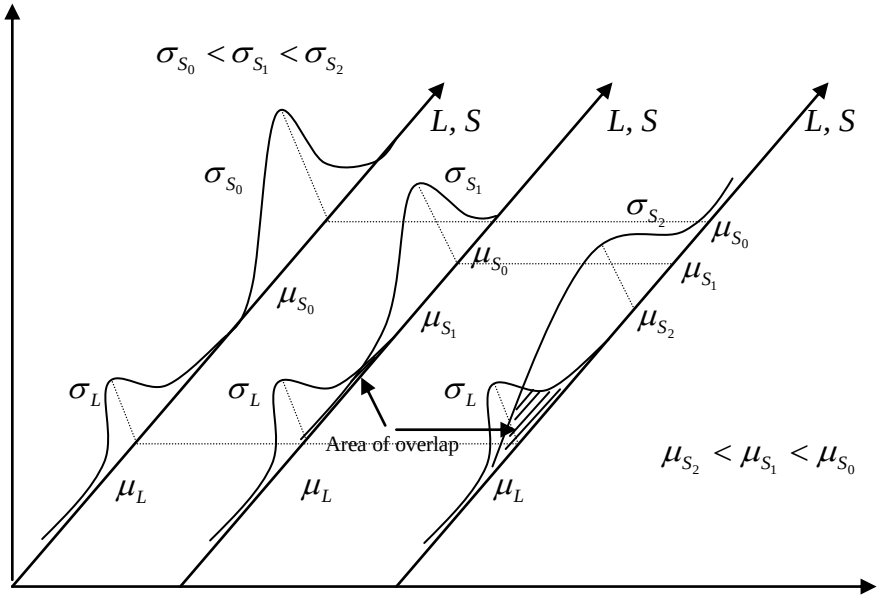

Figure 5: Data acquisition and handling for condition-based maintenance

### 3.2.2 Structures life extension and re-assessment

The possibility of acquiring information on the health state of systems and components is very much of interest for existing structural systems and components, for the assessment of their remaining life.

The assessment of existing structures is usually less formalized than in the design phase of new structures. On the other hand, the reliability model-based assessment of existing structures is gaining considerable interest and there have been a number of practical applications in the areas of offshore structures, bridges and ships (Shinozuka, 1983; Oswald and Schueller, 1984; Myotyri et al., 2006; Schueller and Pradlwarter, 2006). The main motivation for this stems from the need to make proper use of additional 'monitored' information (general impression, results of visual inspection, results of measurements) related to the structure health, from the possibility of building a representative stochastic model of structural behavior and from the opportunity of adopting appropriate levels of target reliability considering the importance of the structure, the consequences of its failure and the cost of its repair (Figure 6). The application in practice of the reliability-based assessment of existing structures is supported by the availability of a number of guidance documents.

Interestingly enough, although the structural reliability analysis methods are equally applicable to industrial plant components, e.g. pressure vessels, process piping etc., their use in the field has been somewhat limited. Something is moving, particularly in the nuclear sector which is taking interest in this for the life extension of their aging plants.




$$0 < t_1 < t_2$$

Figure 6: Degradation of the strength (*S*) of an equipment over time, with respect to a constant load (*L*) (Zio, 2007c)

## 3.3 Complex system analysis: uncertainty

For what we have seen thus far, reliability engineers are continuously challenged by old and new aspects of complexity related to the growth and development of new engineered service and production systems and the corresponding need for adequate methods for their analysis. This technological journey is always accompanied by the 'uncertainty factor' which renders the challenge even more 'exciting'.

Uncertainty is an unavoidable component affecting the behavior of systems and more so with respect to their limits of operation. In spite of how much dedicated effort is put into improving the understanding of systems, components and processes through the collection of representative data, the appropriate characterization, representation, propagation and interpretation of uncertainty will remain a fundamental element of the reliability analysis of any complex system.

With respect to uncertainty, the final objective of reliability analysis and risk assessment is to produce insights in the analysis outcomes which can be meaningfully used by the decision makers. This entails that a number of topics be successfully addressed (Helton, 2004):

- How to collect the information (e.g. in the form of expert judgment) and input it into the proper mathematical format.
- How to aggregate information from multiple, diverse sources into a single representation of uncertainty.
- How to propagate the uncertainty through the model so as to obtain the proper representation of the uncertainty in the output of the analysis.
- How to present and interpret the uncertainty results in a manner that is understandable and useful to decision makers.
- How to perform sensitivity analyses to provide insights with respect to which input uncertainties dominate the output uncertainties, so as to guide resources towards an effective uncertainty reduction.

In view of the above considerations, the proper collection of information by expert judgment will continue to play a relevant role in support to the validity and scientific rigor of reliability analysis. Thus, further advancements in expert judgments analysis are required to render the uncertainty analysis methods robust but at the same time affordable and tailored to the different applications. For example, standardization of the calibration of expert judgments would increase the applicability of the methods (Mosleh, 2007).

Uncertainty can be considered essentially of two different types: randomness due to inherent variability in the system (i.e., in the population of outcomes of its stochastic process of behavior) and imprecision due to lack of knowledge and information on the system. The former type of uncertainty is often referred to as objective, aleatory, stochastic whereas the latter is often referred to as subjective, epistemic, state-of-knowledge (Apostolakis, 1990; Helton, 2004). Whereas epistemic uncertainty can be reduced by acquiring knowledge and information on the system, the aleatory uncertainty cannot and for this reason it is sometimes called irreducible uncertainty.

The distinction between aleatory and epistemic uncertainty plays a particularly important role in the risk assessment framework applied to complex engineered systems such as nuclear power plants. In the context of risk analysis, the aleatory uncertainty is related to the occurrence of the events which define the various possible accident scenarios whereas epistemic uncertainty arises from a lack of knowledge of fixed but poorly known parameter values entering the evaluation of the probabilities and consequences of the accident scenarios (Helton, 2004).

With respect to the treatment of uncertainty, in the current reliability analysis and risk assessment practice both types of uncertainties are represented by means of probability distributions (Aven, 2003). Alternative representations based on different notions of uncertainty are being used and advocated in the context of reliability and risk analysis (Cai, 1996; Da Ruan et al., 2001; Helton, 2004; Soft Methods ESREL, 2007), questioning whether uncertainty can be represented by a single probability or whether imprecise (interval) probabilities are needed for providing a more general representation of uncertainty (Moore, 1979; Coolen, 2004; Coolen and Utkin, 2007; Utkin and Coolen, 2007). It has also been questioned whether probability is limited to special cases of uncertainty regarding binary and precisely defined events only. Suggested alternatives for addressing these cases include fuzzy probability (Zadeh, 1968; Klir and Yuan, 1995; Gudder, 2000) and the concept of possibility (Zadeh, 1965; Unwin, 1986; Dubois and Prade, 1988). Furthermore, probabilities have been criticised for not reflecting properly the weight of the evidence they are based on, as is done in evidence theory (Shafer, 1976).

Evidence and possibility theories, in particular, are similar to probability theory in that they are based on set functions but differ in that they make use of dual set functions. Contrary to probability theory which assigns the probability mass to individual events, the theory of evidence makes basic probability assignments $m(A)$ on sets $A$ (the focal sets) of the power set $P(X)$ of the event space $X$, i.e. on sets of possibilities rather than on single events. This allows the naturally encoding of evidence in favor of the different possibilities which may occur.

Also, probability theory imposes more restrictive conditions on the specification of the likelihood of events as a result of the requirement that the probabilities of the occurrence and nonoccurrence of an event must sum to one. As a result, while in probability theory, a single probability distribution function is introduced to define the probabilities of any event or proposition, represented as a subset of the sample space, in evidence and possibility theory there are two measures of likelihood, belief/plausibility and possibility/necessity, respectively. For example, the evidence theory framework allows for the belief about events and propositions to be represented as intervals, bounded by two values, belief and plausibility. The belief in a proposition is quantified as the sum of the probability masses assigned to all sets enclosed by it, i.e. the sum of the masses of all subsets of the proposition: hence, it is a lower bound representing the amount of belief that directly supports a given proposition at least in part. Plausibility is the sum of the probability masses assigned to all sets whose intersection with the proposition is not empty: hence, it is an upper bound on the possibility that the proposition could be verified, i.e. it measures the fact that the proposition could possibly be true “up to that value” because there is only so much evidence that contradicts it.

Both evidence and possibility theories allow epistemic uncertainty (imprecision) and aleatory uncertainty (variability) to be treated separately within a single framework. Indeed, the corresponding dual fuzzy measures provide mathematical tools to process information which is at the same time of random and imprecise nature (Baudrit et al., 2006; Baraldi and Zio, 2008).

The issue of which framework is best suited for representing the different sources of uncertainty is still controversial and worth of further discussion. A recent critical review of the alternative frameworks of representation of uncertainty is provided in (Flage et al., 2008), from the starting point of view that a full mathematical representation of uncertainty needs to comprise, amongst other features, clear interpretations of the underlying primitive terms, notions and concepts. The review shows that these interpretations can be formulated with varying degrees of simplicity and precision.

# 4 Some remarks on the future needs for the practice of reliability engineering

What are some of the future needs to be addressed for the advancement of reliability engineering in practice?

First of all, the presence of regulatory frameworks can have a determining influence on the use of risk and reliability methods in practice. Indeed, in those industries in which safety requirements are of a prescriptive nature (e.g. the building sector), there is little incentive to invest in expensive reliability/risk studies.

Although regulatory frameworks can definitely be an incentive, a cultural breakthrough is needed for plant owners and system managers to be shown and grasp the benefits obtained from the incurred costs and the time spent in reliability\risk analyses.

To this aim, the availability of codes, standards and good guidance documents is essential for the wider application of risk and reliability methods by practicing engineers. For example, at present there is still a paucity of standards in structural reliability analysis and techniques and this reduces their application for maintenance management (SAFERELNET, 2006b).

Besides, the actual implementation of reliability methods must be supported by reasonably user-friendly software. Several tools are available for standard applications, whereas those advanced issues such as human, software and dynamic reliability need further development of integrated simulation software (Mosleh, 2007).

Finally, lack of good quality and commonly accepted reliability data makes it very difficult to use advanced reliability techniques, even with software available, and raises skepticism about their efficacy in reliability predictions (Blanks, 1998). In this sense, industry-wide efforts need to be undertaken to develop comprehensive database systems (SAFERELNET, 2006b).

# 5 Discussion and outlook: integrated dynamic reliability methodologies

Reliability engineering arouse has a scientific discipline in the 1950s, specialized in the 1960s, was integrated into risk assessment in the 1970s and recognized has a relevant contributor to system analysis with the extensive methodological developments and practical applications of the 1980s and 1990s.

From its infancy, through its childhood and teenage years, reliability engineering has been challenged by three fundamental tasks: system representation and modelling, system model quantification, uncertainty modelling and quantification.

Nowadays, in its maturity of the year 2000s, reliability engineering is still confronted by these challenges, possibly sharpened by the increased complexity of the systems. Indeed, the reliability analysis of the modern complex systems entails an integrated approach in which the hardware, software, organizational and human elements are treated in a combined frame which accounts for their dynamic inter-dependences in the complex related tasks of system production, maintenance and emergency management.

To cope with such complexity, dynamic reliability methodologies are being advocated to provide a framework for simulating directly the response of a system to an initial perturbation, as the system hardware and software components and the operating crew interact with each other and with the environment. This can be achieved by embedding models of controlled process dynamics and human operator behavior within stochastic simulation engines reproducing the occurrence of failure and success transitions along the scenarios.

This way of system modeling goes beyond the classical approach to reliability analysis and risk assessment which relies on techniques, such as event and fault trees, to represent the analyst understanding of the system logic with respect to its failure mechanisms. Such classical approach to system analysis requires significant pre-processing efforts for the analyst to acquire the detailed knowledge of the integral system logic and dynamics necessary to structure the accidental scenarios into the proper discrete logic frame. In some situations this way of approaching the problem fails to capture and reproduce salient features of the system behavior. A typical case is when differences in

the sequence order of the same success and failure events along an accident scenario affect its outcome. Another case is when the timing of occurrence of the events along the scenario substantially affects its evolution and possibly its outcome. Finally, modeling difficulties are encountered when the evolution of the process variables (temperatures, pressures, mass flows, etc …) affects the occurrence probabilities of the events and thus the subsequent scenario evolution.

To cope with these issues, dynamic methodologies attempt to integrate dynamic and stochastic processes to capture the integrated dynamic response of the systems/hardware and software components/operating crew during an accident scenario. In this framework, the analyst is relieved from the preprocessing task of identifying the accident scenarios, which are instead automatically generated within the dynamic simulation, e.g. by means of the Discrete Dynamic Event Trees (DDET) or Monte Carlo (MC) simulation techniques. The basic difference between these two techniques is that in the former all possible scenario branches in the system evolution are exhaustively followed and qualified while in the latter the scenarios are randomly sampled.

The payback for saving in the accident scenario identification task is that the number of scenarios that are analyzed is much larger than that of the classical logic approaches, so that not only the computational burden is increased but also the a posteriori information retrieval and interpretation becomes more difficult.

On the other hand, the dynamic reliability approach brings some clear advantages. First, there is potential for the identification of accident scenarios which may have been overlooked by the analyst in the preprocessing phase. Second, conservative simplifying assumptions made by the analyst, for example on the evolution of some process parameters, can be relaxed as the process evolution is simulated directly by the underlying dynamic model. Finally, additional informative insights become available as a result of the dynamic reliability analysis, in the form of time-dependent probability density functions of components states and process parameters values. In this respect, the amount of information retrievable from dynamic reliability methodologies, in terms of number of scenarios and probability distributions, can be overwhelming and generally calls for a significant effort in the post-processing phase. Yet, retrieving the dominant scenarios of the system dynamic evolution can provide significant safety and reliability insights on the criticality of the scenarios and on the efficiencies of the protections designed to counteract them.

In particular within a Monte Carlo simulation framework for dynamic reliability analysis, the information on the evolution of the system is hidden in the system life histories that are simulated as part of the procedure. Among these histories, there are sequences that reproduce qualitatively similar behaviors in terms of the evolution of the physical parameters and of the sequences of events, mainly differing for the actual times at which these latter occur. Other sequences may

instead differ in behavior, because characterized by different combinations of occurred events, and still reach the same final outcome state. The difficulty in identifying and grouping similar scenarios lies in the fact that same event sequences may correspond to rather different process parameters evolutions and, possibly, end states, depending on the events timing or on their occurrence order. Then, grouping the scenarios only on the basis of the occurred events and end states may not be sufficient and accountancy of the physical behavior of the process variables should also be included.

In any case, in general to be effective the relevant system reliability analyses must be brought into play since the design stage, with continuous feedbacks during operation throughout the system life-cycle. Indeed, the success of the analysis lies in the early and continued understanding of the logics and mechanisms underpinning the system uncertain failure behaviour, which constitute the essential information for striving towards maximum productivity by safe operation, through optimized maintenance and prompt recovery.

The potential for understanding relies on proper tools for the representation of the integrated system, its modelling and quantification in the face of uncertainty. The increased complexity of the engineered systems, with their hardware, software, organizational and human elements and their inter-dependences, potentially increases the uncertainty associated to the systems behaviour and their modelling, for which factual data (on component failure, software failure, human failure, dependent failure, maintenance practice and effects) will continue to be scarce and of poor quality.

In addition, the development of new production and service technologies will continue to foster the emergence of new challenges for the representation, modelling and quantification of the related systems and their failure behaviour.

Finally, there is a new ‘risk’ dimension which poses new challenges to the reliability analysis of systems and their protective barriers: that related to malevolent acts. Security management systems must be invented and implemented, based on analyses conducted with methods which inherit the framework of the classical reliability and risk analysis methods but need to be further extended to cope with the ubiquity of the hazard, particularly for critical infrastructures, the indefiniteness of its nature and the difficulty to clearly identify the most vulnerable system elements in face of a different ‘mechanism of fault injection’, that driven by malevolent acts.

In the gloomy panorama of system behavior analysis above depicted, the sunlight of reliability engineering will fortunately continue to shine because side-by-side to the above old problems and new challenges there is the continuous and strenuous work by the researchers and analysts for adapting and improving the existing methods and for developing and tailoring new ones. As necessary, these efforts embrace multiple directions of battling the difficulties of practical

application through theoretical advancements in system and uncertainty representation and modeling and through computational developments for quantification, the latter particularly sustained by the power of computer simulation.

**Acknowlegments:** The author expresses his gratitude to Professors Aven and Vinnem of the University of Stavanger, Norway, for having provided the opportunity of the plenary lecture at ESREL 2007, which have motivated the considerations contained in this work, and for having solicited and supported the writing of the paper as a follow up of the lecture activity.
Furthermore, the author is indebted with the anonymous referees for their valuable comments which have led to a significant improvement of the paper contents.

# References

(Abdelmoez et al., 2004) Abdelmoez W., Nassar D.M., Shreshevsku M., Gradetsky N., Gunnalan R., Ammar H.H., Yu B. and Mili A., *Error Propagation in Software Architectures*, 10th IEEE International Software Metrics Symposium b(METRICS 2004), 11-17 september 2004, Chicago, USA, IEEE Computer Society, 2004.

(Aggarwal, 1975) Aggarwal K.K., *A simple method for reliability evaluation of a communication system.* IEEE Trans Communication 1975; COM-23: 563-5.

(Albert et al., 2000) Albert R., Jeonh H. and Barabasi A.-L., *Error and Attack Tolerance of Complex Networks*, Nature, Vol. 406, 2000, pp. 378-382.

(Aldemir et al., 1994) Aldemir T., Siu N., Mosleh A., Cacciabue P.C., Goktepe B.G., *Eds.: Reliability and Safety Assessment of Dynamic Process System* NATO-ASI Series F, Vol. 120 Springer-Verlag, Berlin, 1994.

(Alzbutas et al., 2007) Alzbutas R., Izquierdo J.M., Labeau P.E., *Application of Stimulated Dynamics to Probabilistic Safety Assessment*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 2, pp. 1027-1034.

(Apostol, 1969) Apostol T.M., *2nd Ed. Calculus.* Vol. 2, New York, Wiley, 1969

(Apostolakis and Lemon, 2005) Apostolakis G.E., and Lemon D.M., *A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities due to Terrorism*, Risk Analysis, 25, 2005, pp. 361-376.

(Apostolakis, 1990) Apostolakis G.E., *The Concept of Probability in Safety Assessments of Technological Systems*, Science, 1990, pp. 1359-1364.

(Apostolakis, 2006a) Apostolakis G.E., *PRA/QRA: An Historical Perspective*, 2006 Probabilistic/Quantitative Risk Assessment Workshop, 29-30 November 2006, Taiwan.

(Apostolakis, 2006b) Apostolakis G.E., *Recent Regulatory Development in I&C and FIRE Protection in the USA*, Presentation at the Taiwan Atomic Energy Commission, Taiwan, November 2006.

(Ascher and Fengold, 1984) Ascher, H. and Fengold, H., *Repairable Systems Reliability Modelling, Inference, Misconceptions and their Causes*, Marcel Dekker, New York, 1984.

(Aven, 1987) Avent T., *Availability evaluation of oil/gas production and transportation systems*. Reliability Engineering and System Safety, 1987;18:35-44.

(Aven, 1988) Avent T., *Some considerations on reliability theory and its applications*, Reliability Engineering and System Safety, 1988;21:215-23.

(Aven, 1993) Aven, T., *On performance measures for multistate monotone systems*, Reliab. Eng. and Sys. Safety, 1993; 41; 259-266.

(Aven and Jensen, 1999), Aven, T. and Jensen, U., *Stochastic Models in Reliability*, Springer, 1999.

(Aven, 2003) Aven, T., *Foundations of Risk Analysis*, Wiley, 2003.

(Aven et al., 2006) Aven T., Sklet S. And Vinnem J.E., *Barrier and Operational Risk Analysis of Hydrocarbon Release (Bora Release) Part I. Method Description*. Journal of Hazardous Materials A137, 2006, pp. 681-691.

(Barabasi, 2002) Barabasi, A.L., *Linked: The New Science of Networks*, Perseus Publishing, Cambridge, Massachussetts, 2002.

(Baraldi and Zio, 2008) Baraldi P. and Zio E., *A Combined Monte Carlo and Possibilistic Approach to Uncertainty Propagation in Event Tree Analysis*, Risk Analysis 2008.

(Barlow and Proschan, 1975) Barlow, R.E. and Proschan F., *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart and Winston, 1975.

(Bar-Yam, 2000) Bar-Yam, Y., *Dynamics of Complex Systems*, Westview Press, 2002.

(Baudrit and Dubois, 2006) Baudrit C. and Dubois D., *Practical Representations of Incomplete Probabilistic Knowledge*, Computational Statistics and Data Analysis, Vol. 51, 2006, pp. 86-108.

(Baudrit et al., 2006) Baudrit C., Dubois D. and Guyonnet D., *Joint Propagation of Probabilistic and Possibilistic Information in Risk Assessment*, IEEE Transactions on Fuzzy Systems, Vol. 14, 2006, pp. 593-608.

(Bedford and Cooke, 2001) Bedford, T. and Cooke, R., *Probabilistic Risk Analysis*, Cambridge University Press, 2001.

(Bier et al., 2006) Bier, V.M., Gratz, E.M., Haphuriwat, N.J., Magua W. and Wierzibcki K.R., *Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System*, Reliability Engineering and System Safety,92, 2007, pp. 1155-1161.

(Birchmeier, 2007) Birchmeier J., *Systematic Assessment of the Degree of Criticality of Infrastructures*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 859-864.

(Blanks, 1998) Blanks H. S., *The Challenge of Quantitative Reliability*, Quality and Reliability Engineering International, 14, 1998, pp. 167-176.

(Bologna, 2007) Bologna S., *Security of Wide Technological Networks with Particular Reference to Inter-Dependences*, City& Security, Rome, March 30 2007.

(Boring, 2006) Boring R.L., *Modelling Human Reliability Analysis Using MIDAS*, Proceedings of the Fifth International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human Machine Interface Technology, 2006, pp. 1270-1274.

(Boring, 2007) Boring, R.L., *Dynamic Human Reliability Analysis: Benefits and Challenges of Simulating Human Performance*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 2, pp. 1043-1049.

(Braasch et al. 2007) Braasch A., Specht M., Meyna A. Amd Hubner H.-J., *An Approach to Analyze Software Failure Behaviour of Automotive Telecommunication Systems*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 71-75.

(Bye et al. 2006) Bye A., Lauman K., Braarud P.O. and Massaiu S., *Methodology for Improving HRA by Simulator Studies*, Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (PSAM 8), 2006, PSAM-0391, pp. 1-9.

(Cai, 1996) Cai K.-Y., *System Failure Engineering and Fuzzy Methodology. An Introductory Overview*, Fuzzy Sets and Systems 83, 1996, pp. 113-133.

(Capra, 1996) Capra F., *The Web of Life*, Doubleday, New York, 1996.

(Carreras et al., 2002) Carreras B.A., Lynch V., Dobson I., Newman D.E., *Critical Points and Transitions in an Electric Power Transmission Model for Cascading Failure Blackouts*, Chaos, Volume 12, N0. 4, 2002, pp. 985-994)

(Châtelet et al., 2002) Châtelet E., Bérenguer C., Jellouli O., *Performance assessment of complex maintenance policies using stochastic Petri nets*, Proceedings of Esrel'02 - λμ13, Lyon, France, 2002, vol.2, pp. 532-537.

(CNIP, 2006) CNIP'06, *Proceedings of the International Workshop on Complex Network and Infrastructure Protection*, Rome, Italy, 28-29 March 2006.

(Coolen, 2004) Coolen, F.P.A., *On the use of imprecise probabilities in reliability*, Quality and Reliability Engineering International, 2004, 20, pp. 193-202.

(Coolen and Utkin, 2007) Coolen, F.P.A. and Utkin, L.V., *Imprecise probability: A concise overview*, In Aven, T. & Vinnem, J.E. (eds) Risk, reliability and societal safety, Proceedings of the European Safety and Reliability Conference (ESREL), Stavanger, Norway, 25-27 June 2007, London, Taylor & Francis.

Aven, T. 2003. *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*. Chichester: Wiley.

Bedford, T. & Cooke, R.M. 2001. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge: Cambridge University Press.

Bernardo, J.M. & Smith, A.F.M. 1994. *Bayesian Theory*. Chichester: Wiley.

Cai, K.-Y. 1996. *Introduction to Fuzzy Reliability*. Boston: Kluwer.

Dubucs, J.-P. 1993. *Philosophy of Probability*. Dordrecht: Kluwer Academic Publishers.

Gudder, S. 2000. What is fuzzy probability theory? *Foundations of Physics* 30(10): 1663-1678.

Helton, J.C. & Burmaster, D.E. (eds). 1996a. *Reliability Engineering and System Safety* 54(2-3): 91-262. Special issue on treatment of aleatory and epistemic uncertainty.

Helton, J.C. & Burmaster, D.E. 1996b. Guest editorial: treatment of aleatory and epistemic uncertainty in performance assessments for complex systems. *Reliability Engineering and System Safety* 54: 91-94.

Kaplan, S. & Garrick, B.J. 1981. On the quantitative definition of risk. *Risk Analysis* 1(1): 11-27.

Lindley, D.V. 2006. *Understanding Uncertainty*. Hoboken, NJ: Wiley.

Lindley, D.V. 2000. The philosophy of statistics. *The Statistician* 49(3): 293-337.

Natvig, B. 1983. Possibility versus probability. *Fuzzy Sets and Systems* 10: 31-36.

Ross, T.J., Booker, J.M. & Parkinson, J.W. (eds). 2002. *Fuzzy Logic and Probability Applications: Bridging the Gap*. Philadelphia, PA: SIAM.

Shafer, G. 1976. *A Mathematical Theory of Evidence*. Princeton: Princeton University Press.

Shafer, G. 1990. Perspectives on the theory and practice of belief functions. *International Journal of Approximate Reasoning* 4: 323-362.

Singpurwalla, N.D. 2006. *Reliability and Risk: A Bayesian Perspective*. Chichester: Wiley.

Fuzzy Techniques in Reliability. Springer.

Zadeh, L.A. 1965. Fuzzy sets. *Information and Control* 8: 338-353.

Zadeh, L.A. 1968. Probability measures of fuzzy events. *Journal of Mathematical Analysis and Applications* 23: 421-427.

Zadeh, L.A. 1978. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems* 1: 3-28.

(Cooper et al., 1994) Cooper S.E., Ramey-Smith A. M., Wreathall J., Parry G.W., Bley D.C., Luckas W.J., Taylor J.H., Barriere M.T., *A technique for Human Error Analysis (ATHEANA)*, NUREG/CR-6093, U.S. Nuclear Regulatory Commission, Washington DC,1994.

(Coppola, 1984) Coppola A., *Reliability Engineering of electronic Equipment: an Historical Perspective*, IEEE Trans. Reliab., 1984, R-33(1), pp. 29-35.

(Crucitti et al., 2004) Crucitti, P., Latora, V. and Marchiori M., *A Topological Analysis of the Italian Electric Power Grid*, Physica A Vol. 338, 2004, pp. 92-97.

(Da Ruan et al., 2001) Da Ruan, Kacprzyk J. and Fedrizzi M. *Eds., Soft Computing for Risk Evaluation and Management*, Physica-Verlag, 2001.

(Denson, 1998) Denson W., *The History of Reliability Prediction*, IEEE Trans. Reliab. 1998, 47(2-SP), pp. 321-328.

(Dubi, 1998) Dubi, A., *Monte Carlo applications in systems engineering*, John Wiley & sons, 1998

(Dubois and Prade, 1988) Dubois D. and Prade H., *Possibility Theory: An Approach to Computerized Processing of Uncertainty*, New York, Plenum Press, 1988.

(Dubois, 2006) D. Dubois, *Possibility Theory and Statistical Reasoning, Computational Statistics and Data Analysis*, Vol. 51, 2006, pp. 47-69.

(Dutuit et al. 1997) Dutuit Y., Châtelet E., Signoret J.P., Thomas P., *Dependability modelling andevaluation by using stochastic Petri nets: Application to two test cases*, Reliability Engineering and System Safety, 55:117-124, 1997.

(Duval et al., 2007) Duval C., Leger A., Weber P., Levrat E., Lung B., Farret R., *Choice of a Risk Analysis Method for Complex Socio-Technical Systems*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 17-25.

(Engell et al., 1983) Coleridge S.T. *Biographia Literaria*. In: Engell J., Bate W.J., Eds., *The collected works of Samuel Taylor Coleridge*, New Jersey, USA, Princeto University Press, 1983.

(ESReDA, 2007) *Maintenance Modelling and Applications*, Proceedings of the 32nd ESReDA Seminar and 1st ESReDA-ESRA Seminar, 8-9 May 2007, Alghero, Italy.

(EU, 2005) *Green Paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 Final, Brussels, EU, 2005.

(EU, 2006) *European Union Directive Draft*, COM(2006) 787, Brussels, EU, 2006.

(Eusgeld and Kroger, 2008) Eusgeld, I. And Kroger W., *Towards a Framework for Vulnerability Analysis of Interconnected Infrastructures*, Proceedings of the 9th Probabilistic Safety Assessment and Methodology (PSAM 9), Hong Kong, May 19-23, 2008, CD-ROM.

(Farmer, 1964) Farmer, F.R., *The Growth of Reactor Safety Criteria in the United Kingdom*, Anglo-Spanish Power Symposium, Madrid, 1964.

(Flage et al., 2008) Flage, R., Aven, T. and Zio E., *Alternative Representations of Uncertainty in System Risk and Reliability Analysis: Review and Discussion*, Proceedings of ESREL 2008, Valencia Spain, 22-25 September 2008.

(Flin, 2007) Flin R., *Managerial Decisions: Counterbalancing Risks Between Production and Safety*, ESREL 2007 Plenary Lecture, Stavanger, Norway, 26 June 2006 (http://www.esrel2007.com/ ).

(Frankhauser, 2001), Frankhauser, H.R., *Safety Functions versus Control Functions*, Proceedings of 20th International Conference SAFECOM 2001, Budapest, Hungary, Sept. 26-28, 2001.

(Fredriksen and Winther, 2007) Fredriksen R. and Winther R., *Challenges Related to Error Propagation in Software Systems*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 83-90.

(Gandini, 1990) Gandini A., *Importance & Sensitivity analisys in assessing system reliability* IEEE Trans. on Reliab. 1990; vol 39; n. 1, pp 61-69

(Garribba et al., 1985) Garribba S., Guagnini E. and Mussio P., *Multistate block diagrams and fault trees*, IEEE Trans. on Reliab. 1985; vol R-34; n. 5, pp 463-472

(Garrick et al., 1967) Garrick, B.J. and Gekler, W.C., *Reliability Analysis of Nuclear Power Plant Protective Systems*, US Atomic Energy Commission, HN-190, 1967.

(Genetic Algorithms ESREL, 2007) *Genetic Algorithms and Evolutionary Computing for Optimization of RAMS*, Special Sessions I and II, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

(Gran and Thunem, 1998) Gran B.A. and Thunem H., *Experimental Investigation of Software Testing and Reliability Assessment Methods (EISTRAM) Final Report*, Halden Internal Report HWR-528, OECD Halden Reactor Project, April 1998.

(Gregoriades et al., 2003) Gregoriades A., Sutcliffe A. and Shin J.-E., *Assessing the Reliability of Socio-Technical Systems*, Systems Engineering, Vol. 6, No. 3, Vol. 6, 2003, pp. 210-223.

(Griffith, 1980) Griffith, W. S., *Multistate reliability models*, Journal of Applied Probability, Vol. 17 (1980), pp. 735-744.

(Gudder, 2000) Gudder, S., What is fuzzy probability theory? *Foundations of Physics* 30(10), 2000, pp. 1663-1678.

(Haarla et al., 2008) Haarla, L., Pulkkinen, U., Koskinen M. And Jyrinsalo J., *A Method for Analysing the Reliability of a Transmission Grid*, Reliability Engineering and System Safety, 93, 2008, pp. 277-287.

(Hannaman et al., 1984) Hannaman G., Spurgin A., Lukic Y., *Human cognitive reliability model for PRA analysis*, Technical report NUS-4531, Palo Alto California Electric Power Research Institute, 1984.

(Hannaman et al., 1985) Hannaman G., Spurgin A., Lukic Y., *A model for assessing Human Cognitive Reliability in PRA studies*, IEEE Third Conference on Human Factors in Nuclear Power Plants, Monterey, California, June 23-27, 1985. Institute of Electronic and Electrical Engineers, New York (USA), 1985.

(Helton, 2004) Helton J.C., *Alternative Representations of Epistemic Uncertainty*, Special Issue of Reliability Engineering and System Safety, Vol. 85, 2004.

(Henley and Kumamoto, 1992) Henley, E.J. and Kumamoto, H., *Probabilistic risk assessment*, NY, IEEE Press, 1992.

(Hiller et al., 2001) Hiller M., Jhumka A. And Suri N., *An Approach for Analyzing the Propagation of Data Errors in Software*, Dependable Systems and Networks, 2001, pp. 161-170.

(Hiller et al, 2001) Hiller M., Jhumka A. And Suri N., *PROPANE: An Environment for Examining the Propagation of Errors in Software*, International Symposium on software Testing and Analysis (ISSTA), 2002, pp. 81-85.

(Hollnagel, 1998) Hollnagel E., *Cognitive reliability and error analysis method (CREAM)*, Elsevier Science Ltd., 1998.

(Hollnagel et al., 2006) Holnagel, E., Woods, D.D. and Leveson, N., Eds., *Resilience Engineeering: Concepts and Precepts*, Aldershot, UK: Ashgate, 2006.

(Hokstad and Corneliussen, 2004) Hokstad, P. and Corneliussen K., *Loss of Safety Assessment and the IEC 61508 Standard*, Reliability Engineering & System Safety, 83, 2004, Pages 111-120.

(Horton, 1992) Horton, M., Optimum maintenance and RCM. In *Proc. 3rd EsReDa Seminar on Equipment Aging and Maintenance*, Chamonix, France, 14-15 Oct. 1992.

(Hurst et al., 1992) Hurst N.W., Bellamy L.J., Geyer T.A. and Astley J.A., *A Classification Scheme for Pipework Failures to Include Human and Socio-Technical Errors and Their Contribution to Pipework Failure Frequencies*, Journal of Hazardous Materials, 26, 1991, pp. 159-186.

(IRGC, 2006) *White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*. International Risk Governance Council, Geneva, 2006.

(Jae and Park, 1995) Jae M.S. and Park C.K., *A New Dynamic HRA Method and its Application*, Journal of the Korean Nuclear Society, 1995, 27, pp. 292-300.

(Jane et al., 1993) Jane CC, Lin JS, Yuan J., *Reliability evaluation of a limited-flow network in terms of MC sets*, IEEE Trans Reliability, 1993;R-42:354-61.

(Jarrell et al., 2004) Jarrell D.B., Sisk D. R. and Bond L.J., *Prognostics and Condition-Based Maintenance: A New Approach to Precursive Metrics*, Nuclear Technology, Vol. 145, 2004, pp. 275-286.

(Jonsson et al. 2007) Jonsson H., Johansson J. and Joansson H., *Identifying Critical Components in Electric Power Systems: A Network Analytic Approach*, Proceedings of ESREL 2007, Stavanger, Norway, pp. 889-897.

(Jovanovic, 2003) A. Jovanovic, *Risk-Based Inspection and Maintenance in Power and Process Plants in Europe*, Nuclear Engineering and Design 226, 2003, pp. 165-182.

(Kaplan and Garrick, 1984) Kaplan, S. and Garrick, B. J., *Risk Analysis, 1*, p. 1-11, 1984.

(Kastenberg, 2005) Kastenberg, W.E., *Assessing and Managing the Security of Complex Systems: Shifting the RAMS Paradigm*, Proceedings of the 29th ESReDA Seminar on Systems Analysis for a more Secure World, JRC-IPSC, Ispra, Italy, October 25-26, 2005, pp. 111-126.

(Kauffman, 1993) Kauffman, S.A., *The Origins of Order*, Oxford University Press, 1993.

(Klir and Yuan, 1995) Klir G.J., Yuan B., *Fuzzy Sets and Fuzzy Logic: Theory and Applications*, Prentice Hall, 1995.

(Koonce et al., 2007) Koonce, A.M., Apostolakis, G.E. and Cook, B.K., *Bulk Power Risk Analysis: Ranking Infrastructure Elements According to their Risk Significance*, Electricap Power and Energy Systems, 2007.

(Korbicz et al., 2004) Korbicz J., Koscielny J.M., Kowalczuk Z. and Cholewa W., *Eds., Fault Diagnosis*, Springer, 2004.

(Kubat, 1989) Kubat P., *Estimation of reliability for communication/computer networks simulation/analytical approach*. IEEE Trans Communication, 1989; 37:927-33.

(Labeau and Zio, 2001) Labeau P., Zio E., *Biasing Schemes in Component-based and System-based Monte Carlo Algorithms in System Engineering*, Proceedings of ESREL 2001 European Safety and Reliability Conference, September 16-20, 2001, Torino, Italy, pp. 903-910.

(Larsen et al., 2000) Larsen K. G., Nielsen M. and Thiagarajan P.S., *Timed and Hybrid Automata*, 2nd International Conference on Application and Theory of Petri Nets, Aarhus, Denmark, June 26-30, 2000.

(Lisnianski and Levitin, 2003) Lisnianski A., Levitin G., *Multi-state system reliability*. Assessment, Optimization and Applications, World Scientific, 2003.

(Maintenance ESREL, 2007) *Managing Maintenance for Improving Safety and Production*, Special Sessions I and II, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

(Marseguerra and Zio, 1993) Marseguerra M., Zio E., *Nonlinear Monte Carlo Reliability Analysis with Biasing Towards Top Event*, Reliability Engineering and System Safety 40, pp. 31 - 42, 1993.

(Marseguerra and Zio, 2000) Marseguerra M., Zio E., *System Unavailability Calculations in Biased Monte Carlo Simulation: a Possible Pitfall*, Annals of Nuclear Energy, 27, 2000, pp. 1589 - 1605.

(Marseguerra and Zio, 2000) Marseguerra M., Zio E., *Optimizing Maintenance and Repair Policies via a Combination of Genetic Algorithms and Monte Carlo Simulation*, Reliability Engineering and System Safety, 68, 2000, pp. 69 - 83.

(Marseguerra and Zio, 2002) Marseguerra M, Zio E., *Basics of the Monte Carlo Method with Application to System Reliability*. LiLoLe- Verlag GmbH (Publ. Co. Ltd.), 2002

(Marseguerra et al., 2006) Marseguerra M., Zio E., Martorell S., *Basics of Genetic Algorithms Optimization for RAMS Applications*, Reliability Engineering and System Safety, 91, 2006, pp. 977-991.

(McCormick, 1981) McCormick, N.J., *Reliability and risk analysis*, New York, Academic Press, 1981.

(Michaud and Apostolakis, 2006) Michaud, D. and Apostolakis G.E., *Methodology for Ranking the Elements of Water-Supply Networks*, Journal of Infrastructure Systems, 2006, pp. 230-242.

(Monden, 1998) Monden Y., *Toyota Production Systems*. Industrial Engineering and Management Press, Norcross, GA, 1998

(Moore, 1979) Moore R.E., *Methods and Applications of Interval Analysis*, Philapdelphia, PA: SIAM, 1979.

(Moranda, 1975) Moranda P.B., *Prediction of Software Reliability During Debugging*, Proc. Ann. Reliab. Maintain. Symp., 1975, pp. 327-332.

(Mosleh, 2007) Mosleh A., *Next Generation Risk Methods*, ESREL 2007 Plenary Lecture, Stavanger, Norway, 25 June 2006 (http://www.esrel2007.com/ ).

(Mosleh and Chang, 2004) Mosleh A. and Chang Y.H., *Model-Based Human Reliability Analysis: Prospects and Requirements*, Reliability Engineering and system Safety, 2004, 83, pp. 241-253.

(Murphy and Pate-Cornell, 1996) Murphy D.M and Pate-Cornell M.E., *The SAM Framework: Modelling the Effects of Management Factors on Human Behaviour in Risk analysis*, Risk Analysis, 16, 1996, pp. 501-515.

(Myotyri et al., 2006) Myotyri E., Pulkkinen U. and Simola K., *Application of Stochastic Filtering for Lifetime Prediction*, Reliability Engineering and System Safety, 91, 2006, pp. 200-208.

(NASA, 2002) *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, NASA, 2002.

(Nowlan and Heap, 1978), Nowlan, F.S. and Heap, H.F., *Reliability-centered Maintenance*, Technical Report AD/A066-579. National Technical Information Service, US Department of Commerce, Springfield, Virginia, 1978.

(NUREG/CR-2300, 1983) *PRA Procedures Guide*, Vols. 1&2, NUREG/CR-2300, January 1983.

(NUREG/CR-6901, 2006) *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, US NRC, 2006.

(Oh et al, 1998) Oh J.I.H., Brouwer W.G.J., Bellamy L.J., Hale A.R., Ale B. and Papazoglou I.A., *The I-Risk Project: Development of an Integrated Technical and Management Risk Control and Monitoring Methodology for Managing and Quantifying On-Site and Off-Site Risks*. In: Mosleh A.

and Bari R. Eds., Proc. Od the International Conference on Probabilistic Safety Assessment and Management 4 (PSAM 4), New York, Springer, 1998, pp. 2485-2491.

(OHS, 2002) *National Strategy for Homeland Security*, US Office of Homeland Security, Washington, 2002.

(Oien, 2001) Oien K., *A Framework for the Establishment of Organisational Risk Indicators*, Reliability Engineering and System Safety, 74, 2001, pp. 147-167.

(Oswald and Schueller, 1984) Oswald G.F. and Schueller G.I., *Reliability of Deteriorating Structures*, Fracture Mechanics, Vol. 20, No. 3, 1984, pp. 479-488.

(Parikh et al., 2001) Parikh C.R., Pont M.J. and Jones N.B., *Application of Dempster-Shafer theory in condition monitoring systems: A case study*, Pattern Recognition Letters, Vol. 22 no.6-7, 2001, pp. 777-785

(Patterson and Apostolakis, 2007) Patterson, S.A. and Apostolakis, G.E., *Identification of Critical Locations across Multiple Infrastructures for Terrorist Actions*, Reliability Engineering and System Safety, 92, 2007, pp. 1183-1203.

(Poszgai and Bertsche, 2003) Poszgai P., Bertsche B., *On the influence of the passive states on the availability of mechanical systems*, Safety and Reliability-Bedford & van Gelder (eds), 2003, 1255-1262.

(Production Assurance ESREL, 2007) *Production Assurance Special Sessions I and II*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

(Rankin and Krichbaum, 1998) Rankin W. and Krichbaum L., *Human Factors in Aircraft Maintenance. Integration of Recent HRA Developments with Applications to Maintenance in Aircraft and Nuclear Settings*. Seattle. Washington. USA.

(Rausand, 1998) Rausand, M., *Reliability Centered Maintenance.* Reliability Engineering and System Safety, 60, 1998, 112 - 132.

(Raymond Knight, 1991) Raymond Knight C., *Four Decades of Reliability Progress*. Proceedings of the Annual Reliability and Maintainability Symposium, IEEE 1991, pp. 156-160.

(Reason, 1998) Reason J., *Managing the Risks of Organisational Accidents*, Ashgate Publishing Ltd., Aldershot.

(Reer et al., 2004) Reer B., Dang V.N. and Hirschberg S., *The CESA Method and its Application in a Plant-Specific Pilot Study on Errors of Commission*, Reliability Engineering and System Safety, 2004, 83, pp. 187-205.

(Rocco et al., 2007) Rocco C. M., Zio E. and Salazar D.E., *Multi-objective Evolutionary Optimisation of the Protection of Complex Networks Exposed to Terrorist Hazard*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 899-905.

(Rosato et al., 2007) Rosato V., Bologna S. and Tiriticco F., *Topological Properties of High-Voltage Electrical Transmission Networks*, Electric Power Systems Research, 77, 2007, pp. 99-105.

(Roverso et al., 2007) Roverso D., Hoffmann M., Zio E., Baraldi P., Gola G., *Solutions for Plant-Wide On-Line Calibration Monitoring*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 827-832.

(Sachdeva, 2007) Sachdeva A., Kumar D. and Kumar P., *Reliability Modeling of an Industrial System with Petri Nets*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 2, pp. 1087-1094.

(SAFERELNET, 2006a) *Framework Document on Maintenance Management*, 2006, http://www.mar.ist.utl.pt/saferelnet/ .

(SAFERELNET, 2006b) *Safety and Reliability of Industrial Products, Systems and Structures – Current Position and Future Research Needs*, 2006, http://www.mar.ist.utl.pt/saferelnet/ .

(Saleh and Marais, 2006) Saleh J.H. and Marais K., *Highlights from the Early (and Pre-) History of Reliability Engineering*, Reliability Engineering and System Safety 91, 2006, pp. 249-256.

(Salmeron et al., 2004) Salmeron, J., Wood, K. and Baldick R., *Analysis of Electric Grid Security Under Terrorist Threat*, IEEE Trans. On Power Systems, Vol. 19, No. 2, 2004, pp. 905-912.

(Samad, 1987) Samad MA., *An efficient algorithm for simultaneously deducing MPs as well as cuts of a communication network*. Microelectronic Reliability, 1987; 27:437-41.

(Schneeweiss, 2004) Schneeweiss W.G., *Petri Net Picture Book*, LiLoLe-Verlag GmbH, 2004.

(Schueller and Pradlwarter, 2006) Schueller G. I. and Pradlwarter H. J., *Computational Stochastic Structural Analysis (COSSAN) – A Software Tool*, Structural Safety 28, 2006, pp. 68-82.

(Science, 1999) Science, *Special Section on Complex Systems*, Volume 284, No. 5411, April 2, 1999, pp. 79-109.

(Shafer, 1976) Shafer G., *A Mathematical Theory of Evidence*, Princeton, NJ: Princeton University Press, 1976.

(Schlapfer et al., 2008) Schläpfer M., Kessler T. and Kröger W., *Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach*, 16th Power Systems Computation Conference, Glasgow, 2008.

(Shinozouka, 1983) Shinozouka M., *Basic Analysis of Structural Safety*, Journal of Structural Engineering, Vol. 10, No. 3, 1983.

(Soft Methods ESREL, 2007) *Soft Methods in Safety and Reliability*, Special Sessions I-III, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

(Software Reliability ESREL, 2007) *Software Reliability*, Special Session, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 2.

(Strater, 2005) Strater O., *Cognition and Safety: An Integrated Approach to Systems Design and Performance Assessment*, Aldershot: Ashgate, 2005.

(Swain and Guttman, 1983) Swain A.D., Guttman H.E., *Handbook of human reliability analysis with emphasis on nuclear power plant applications*, NUREG/CR-1278, 1983.

(Swain, 1987) Swain A.D., *Accident sequence evaluation program human reliability analysis procedure*, NUREG/CR-4772, 1987.

(Trbojevic et al., 2007) Trbojevic V.M, Gudmestad O.T. and Rettedal W.K., *Accounting for Management and Organisational Factors in Risk Analysis of Marine Operations*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 51-60.

(Trucco et al., 2006) Trucco P., Leva M.C. and Strater O., *Human Error Prediction in ATM via Cognitive Simulation: Preliminary Study*. Proceedings of the 8th International Conference on Probabilistic Safety Assesment and Management (PSAM 8), 2006, PSAM-0268, pp. 1-9.

(van Rijn, 2007) van Rijn, Cyp F.H., *Maintenance Modeling and Applications; Lessons Learned*, Proceedings of the 32nd ESReDA Seminar and 1st ESReDA-ESRA Seminar, 8-9 May 2007, Alghero, Italy, pp. 1-24.

(Unwin, 1986) Unwin, S.D., A *fuzzy set theoretic foundation for vagueness in uncertainty analysis*, Risk Analysis 6(1), 1986, pp. 27-34.

(Utkin and Coolen, 2007) Utkin, L.V. and Coolen, F.P.A., *Imprecise reliability: An introductory overview*, In Levitin, G. (ed.) Computational Intelligence in Reliability Engineering – New Metaheuristics, Neural and Fuzzy Techniques in Reliability, Springer, 2007.

(Vinnem, 2007) Vinnem J.E., Seljelid J., Haugen S., Sklet S., Aven T., *Generalised Methodology for Operational Risk Analysis*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 61-68.

(Voas, 1997) Voas J., *Error Propagation Analysis for COTS Systems*, IEEE Computing and Control Engineering Journal, 8(6), 1997, pp. 269-272.

(Vulnerability ESREL, 2007) *Vulnerability, Reliability and safety of Complex Networks and Critical Infrastructures*, Special Sessions I and II, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

(WASH-1400, 1975) WASH-1400, *Reactor Safety Study*, US Nuclear Regulatory Commission 1975.

(Wood, 1985) Wood A. P., *Multistate block diagrams and fault trees*, IEEE Trans. on Reliab. 1985; vol R-34; n. 3, pp 236-240.

(Wreathall et al., 1992) Wreathall J., Schurman D.L., Modarres M., Anderson N., Roush M.L. and Mosleh A., *US Regulatory Commission: A Framework and Method for the Amalgamation of*

*Performance Indicators at Nuclear Power Plants*. Report NUREG-5610, Vols. 1 and 2, 1992, US Nuclear Regulatory Commission, Washington DC, USA.

(Yeh, 1995) Yeh, L., *Calculating the Rate of Occurrence of Failures for Continuous-Time Markov Chains with Application to a Two-Component Parallel System*, Journal of the Operational Research Society, 1195, 46, pp. 528-536.

(Yeh, 1998) Yeh W.C., Revised A., *Layered-network algorithm to search for all d-minpaths of a limited-flow acyclic network*. IEEE Trans Reliability, 1998; R-46:436-42.

(Zadeh, 1965) Zadeh L.A., *Fuzzy Sets*, Information and Control, Vol. 8, 1965, pp. 338-353.

(Zadeh, 1968) Zadeh, L.A., *Probability measures of fuzzy events*, Journal of Mathematical Analysis and Applications, 23, 1968, pp. 421-427.

(Zadeh, 1978) Zadeh, L.A., *Fuzzy sets as a basis for a theory of possibility*, Fuzzy Sets and Systems, 1, 1978, pp. 3-28.

(Zille et al., 2007) Zille V., Berenguer C., Grall A., Despujols A., Lonchampt J., *Modelling and Performance Assessment of Complex Maintenance Programs for Multi-Component Systems*, Proceedings of the 32nd ESReDA Seminar and 1st ESReDA-ESRA Seminar, 8-9 May 2007, Alghero, Italy, pp. 127-140.

(Zio et al., 2006) Zio E., Baraldi P., Patelli E., *Assessing the Availability of an Offshore Installation by Monte Carlo Simulation*, International Journal of Pressure Vessel and Piping, 83, 2006, pp. 312-320.

(Zio et al., 2007a) Zio E., Marella M. and Podofillini L., *A Monte Carlo Simulation Approach to the Availability Assessment of Multi-State Systems with Operational Dependencies*, Reliability Engineering and System Safety, 92, 2007, pp. 871-882.

(Zio et al., 2007b) Zio E., Baraldi P., Librizzi M., *A Fuzzy Logic Model for the Assessment of Crew Performance in Simulated Scenarios*, Internal Report, 2007.

(Zio et al., 2007 c) Zio E., Baraldi P., Librizzi M., L. Podofillini, V.N. Dang, *A Fuzzy Expert System for Modelling Dependence among Human Errors*, Accepted for publication on Fuzzy Sets and Systems, 2007.

(Zio, 2007a) Zio E., *From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures*, Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, 2007, pp. 488-508.

(Zio, 2007b) Zio E., *Soft Computing Methods applied to condition monitoring and fault diagnosis for maintenance*, Proceedings of the Summer Safety and Reliability Seminars, Gdansk/Sopot-Jelitkowo, Poland, July 22-29, 2007.

(Zio, 2007c) Zio E., *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific Publishing, 2007.