Accepted Manuscript

The Future of Risk Assessment

E. Zio

PII: S0951-8320(17)30654-3
DOI: 10.1016/j.ress.2018.04.020
Reference: RESS 6139

To appear in: *Reliability Engineering and System Safety*

Received date: 1 June 2017
Revised date: 20 March 2018
Accepted date: 24 April 2018

Please cite this article as: E. Zio , The Future of Risk Assessment , *Reliability Engineering and System Safety* (2018), doi: 10.1016/j.ress.2018.04.020

Highlights

- A view on the future of risk assessment is provided
- Research directions are presented on the use of simulation for accident scenario identification and exploration
- The use of data for condition monitoring-based, dynamic risk assessment is discussed
- The extension of risk assessment into the framework of resilience and business continuity is presented
- The directions for and integrated safety and security assessment of CPSs are discussed

The Future of Risk Assessment

E. Zio

Chaire Systems Science and the Energy Challenge, Fondation Electricité de France (EDF), Laboratoire Genie Industriel, CentraleSupélec, Université Paris-Saclay, Grande voie des Vignes, 92290 Chatenay-Malabry, France

Energy Department, Politecnico di Milano, Via La Masa 34, Milano, 20156, Italy

Corresponding author: enrico.zio@polimi.it, enrico.zio@centralesupelec.fr

ABSTRACT:

Risk assessment must evolve for addressing the existing and future challenges, and considering the new systems and innovations that have already arrived in our lives and that are coming ahead. In this paper, I swing on the rapid changes and innovations that the World that we live in is experiencing, and analyze them with respect to the challenges that these pose to the field of risk assessment. Digitalization brings opportunities but with it comes also the complexity of cyber-phyiscal systems. Climate change and extreme natural events are increasingly threatening our infrastructures; terrorist and malevolent threats are posing severe concerns for the security of our systems and lives. These sources of hazard are extremely uncertain and, thus, difficult to describe and model quantitatively.

Some research and development directions that are emerging are presented and discussed, also considering the ever increasing computational capabilities and data availability. These include the use of simulation for accident scenario identification and exploration, the extension of risk assessment into the framework of resilience and business continuity, the reliance on data for dynamic and condition monitoring-based risk assessment, the safety and security assessment of cyber-physical systems.

The paper is not a research work and not exactly a review or a state of the art work, but rather it offers a lookout on risk assessment, open to consideration and discussion, as it cannot pretend to give an absolute point of view nor to be complete in the issues addressed (and the related literature referenced to).

KEYWORD: Risk assessment, Simulation, Business continuity, Resilience, Condition monitoring-based risk assessment, Dynamic risk assessment, Cyber-physical systems, Safety and security assessment.

1 Introduction

Safety is freedom, freedom from unaffordable harm, and, thus, a human right. Risk assessment has been the dominant paradigm for ensuring this right in the design and operation of industrial systems. Examples of areas of applications include the chemical process industry, the nuclear industry, the transportation sectors, the aerospace industry etc.

Risk assessment is a mature discipline. The structured performance of a risk assessment guides analysts to identify possible hazards/threats, analyze their causes and consequences, and describe risk, typically quantitatively and with a proper representation of uncertainties. In the assessment, the analysts make assumptions and simplifications, collect and analyze data, and develop and use models to represent the phenomena studied. For example, the failure modes of components due to a given earthquake, the heat fluxes on a structure due to a fire, the response of operators to an accident are all the results of conceptual models that attempt to mimic how a real accident would proceed, based on the knowledge available. The risk assessment of a system requires the consideration of a possibly very large number of scenarios with multiple failures of its components and, by so doing, provides an in-depth understanding and knowledge of the system failure modes with consequent increase of the awareness on risk and the attention to safety, which typically leads to an overall improvement of the safety of the system.

The World we live in is rapidly changing in many ways. Digitalization is bringing new opportunities of connectivity, monitoring and awareness, and is changing the way we communicate and socially behave. Mobility and social pressure are changing the landscape in which we live and operate. Continuous advancements in technical knowledge and technology are improving our production processes, products and services, as well as our environments, while changing the business and work/job scenarios. As the digital, physical and human worlds continue to integrate, we experience a deep transformation in industry, which far-reaches into our lives. The 4th industrial revolution, the internet of things and big data, the industrial internet, are changing the way we design, manufacture, supply products and services, the way we move and live in our environment. This is creating a complex network of things and people that are seamlessly connected and communicating. It is providing opportunities to make production systems and services more efficient and faster, and more flexible and resilient the complex supply chains and distribution networks that tie the global economy.

In this fast-pace changing environment, the attributes related to the reliability of components and systems continue to play a fundamental role for industry and those of safety and security are of increasing concern, as a right to freedom. The innovations that are being developed have high potential of increased wellbeing and benefits, but also generate new failure mechanisms and hazards, and create new risks, partly due also to new and unknown functional and structural dependencies in and among the systems. On the other hand, the advancements in knowledge, methods and techniques, the increase in information sharing, data availability and computational capabilities, and the advancements in knowledge that these can bring, offer new opportunities of development for the analysis and assessment of risks. An evolution of risk assessment is in the making, or perhaps even a “revolution” that takes the form of new approaches to and methods for risk assessment.

In this paper, I consider the above context and point at some directions that are shaping the road of advancement of risk assessment. The underlying perspective taken stands on:

- the recognition that the knowledge, information and data (KID) available for analyzing and characterizing hazards, modeling and computing risk are substantially grown and continue to do so;
- the evidence that the modeling capabilities and computational power available have

significantly advanced and allow unprecedented analysis with previously infeasible methods;

- the concern that the increased complexity of the systems, nowadays more and more made of heterogeneous elements (hardware, human, digital) organized in highly interconnected structures, leads to behaviors that are difficult to anticipate or predict, driven by unexpected events and corresponding emerging unknown systems responses;
- the realization that to manage risk in a systematic and effective way it is necessary to consider together all phases of the potential accident scenarios that may occur, including prevention, mitigation, emergency crisis management and restoration, and that this entails an extended vision of risk assessment for an integrated framework of business continuity (with respect to production reliability and availability) and resilience (with respect also to safety);
- the acknowledgment that risk varies significantly over time and so may also the conditions and effectiveness of the prevention, protection and mitigation measures installed;
- the consideration of the need of solid frameworks for the safety and security assessment of cyber-phyiscal systems (CPSs).

As the future seems to have already arrived and considering that the roots of the methodologies to deal with the associated risks can be found in the past, in the following Sections some directions and challenges for risk assessment are discussed in relation to simulation for accident scenario identification and exploration, resilience and business continuity, dynamic and condition monitoring-based risk assessment, CPSs and their safety and security assessment.

2 Risk Assessment

Industry is undergoing rapid changes in technology and business management. Competitiveness and liberalization have brought considerable advantages in the quality of products and services. On the other hand, processes and systems have seen an increase in the complexity of their operation (energy ratings have increased, pressures, temperatures, flows have increased, storages have been reduced, interdependencies among industries and technologies have increased, particularly through digitalization and information sharing, etc.). As a result, hazards have changed and risk of large scale accidents with significant losses in both human lives and economic terms has increased. This has led to growing public concern to safety and protection from industrial (and natural) disasters, with consequential increased intensity in safety regulation and in the scrutiny of safety procedures.

In this evolving scenario, risk assessment remains a fundamental technical framework for the systemic analysis of the risk associated to an industrial activity. The aim is to acquire a proper understanding of the issues involved, so as to be able to take confident risk-informed decisions for protecting from such risk.

The underlying principles of risk assessment are captured in the National Academy of Science "Red Book", where the two activities of assessment and decision making are kept distinct: assessment of risk is treated as a scientific activity limited by the available knowledge and the uncertainty inherent in risk, and decision making based on risk is regarded as a political activity, with the outcomes of risk assessment being one type of input but never the sole basis for decision making (National Academy Press 1983). Risk as a numerical quantity is, then, useful for making decisions such as on risk prevention and mitigation measures, prioritizing measures on different sources of risk, regulating and accepting risk, transferring risk through insurance. Then, again, risk assessment should be considered as a tool for safety analysis that supports safety-related, rational decision making.

Risk assessment is a science that has been developed in the past 40 years to help understanding and controlling the risk of accident events. This allows the rational management of hazardous industrial activities, through their systemic understanding. The accident events for which the assessment is made are typically extreme but also very unlikely. The rarity of these events is such that there is typically very little 'statistical' information associated to their occurrence. The challenge is, then, to lay down all the knowledge available about these rare but potentially disastrous accident events, often coming from expert judgment supported by indirect physical observations (e.g. the measurement of the duct wall thickness in a pipeline) and model predictions (e.g. the prediction of the crack propagation in a turbine). The basic idea of risk assessment is to structure, by systematic modelling, the information and knowledge available at the detailed component/basic event level to assess the accident risk at system level. As knowledge on these events and on the system responses to them is limited, the outcomes of the assessment are uncertain. The common framework used to describe the uncertainties in the assessment stands on probability theory, and particularly on the subjectivistic (Bayesian) theory of probability, as the adequate framework within which expert opinions can be combined with statistical data to provide quantitative measures of risk (Kelly and Smith; 2009, 2011). Indeed, the common term used is Probabilistic Risk Assessment (PRA), although Probabilistic Safety Assessment (PSA) and Quantitative Risk Assessment (QRA) are also widely used.

For more than 35 years, the probabilistic analysis has provided the basis for the quantification of risk (see reviews by Rechard (1999, 2000)), with its first application to large technological systems (specifically nuclear power plants) dating back to the early 1970s (NRC 1975). The basic principles underpinning today's analyses have not much changed since. However, the purely probability-based approaches to risk assessment are challenged when dealing with highly unlikely industrial accidents (with extreme consequences). For these rare events, only very limited knowledge exists in support to the risk assessment and a number of alternative frameworks for uncertainty representation and treatment in risk assessment have been introduced (Aven and Zio 2011; Dubois 2010, Baraldi, Flage, Aven and Zio 2014; Ahn and Yang, 2003; Kang et al. 2016).

From a general point of view, the concept of risk is introduced to deal with the possibility that an event or situation with undesirable consequences for some subjects may occur. The consequences are often seen in relation to some reference values (planned values, objectives, etc.) and the focus is tyipically on negative consequences. Correspondingly, the International Risk Governance Council (IRGC) defines risk as an uncertain (generally adverse) consequence of an event or activity with respect to something that human beings value (IRGC, 2012). Various similar definitions of risk can be found in the glossary of the Society for Risk Analysis (SRA) Specialty Group on foundational issues in risk analysis (http://www.sra.org/frasg). Detailed scenarios are, then, commonly defined when involved subjects treat "a risk", i.e. a specific risk described in terms of originating hazardous conditions and undesirable consequences for the subjects. For the purposes of formal analysis and with the aim of quantification, formal characterizations and representations of risk are, then, adopted. One common description is (Kaplan & Garrick, 1981):

$$Risk = \{\langle s_i, \not{f}_i, c_i \rangle\},\ i = 1, \dots, N \tag{1}$$

where s_i represents the sequence of events of the i-th of N accident scenarios, $\not{f}_i$ represents the frequency of occurrence of such a sequence of events and c_i is the consequence that would result if that scenario were to occur. For risk assessment in practice, this definition leads to the need of developing methods for the identification of the complete set of accident scenarios that could occur, and the accurate estimation of their frequencies of occurrence and consequences. As completeness of scenarios cannot be guaranteed and accuracy of estimation must be evaluated in the face of limited knowledge and approximated modelling, a second-level definition of risk needs to be introduced to account for the uncertainties associated to the risk assessment (Kaplan & Garrick, 1981):

$$Risk = \{\langle s_i, p_i(\not{f}_i, c_i)\rangle\},\ i = 1, \dots, N+1 \tag{2}$$

where, $p_i(.,.)$ is a joint probability density function describing the uncertainties on the frequency of occurrence $\not{f}_i$ and the consequences c_i of accident scenario s_i, and the *N+1* scenario is added to account for the incompleteness of the set of scenarios, i.e., for those scenarios that have not been considered because unknown at the time of the analysis (i.e., the so-called "residual risk").

As knowledge is central to the risk assessment, the definition of risk can be extended to make it explicit (Aven 2010):

$$Risk = (\mathcal{A}, \mathcal{C}, \mathcal{Q}; \mathcal{K}) \tag{3}$$

where $\mathcal{A}$ indicates the set of accident scenarios that may occur, $\mathcal{C}$ represents the set of consequences, $\mathcal{Q}$ is the metric used to quantify the associated uncertainties and $\mathcal{K}$ is the body of knowledge which the risk assessment (i.e., the identification of $\mathcal{A}$ and the quantification of $\mathcal{C}$ and $\mathcal{Q}$) is based on. This is coherent with the model of the world introduced in (Apostolakis 1990), conditional on the entire body of knowledge and beliefs of the modeler. Note that the formulation in (3) does not restrict the representation of the uncertainty to the classical probabilistic one and alternative representations can be employed (Aven, 2011; Aven, Baraldi, Flage, & Zio 2014; Dubois 2006; Flage, Aven, Zio, & Baraldi 2014; Pedroni, Zio, Pasanisi, & Couplet 2017).

This formulation underlines explicitly the role of the background knowledge systematically incorporated in the risk assessment model; it makes it explicit that the risk assessment outcomes are functions of the current state of knowledge, and of the related assumptions made and parameter values assigned. Recognizing this simple fact has become so important that the need as arisen of explicitly specifying the concept that risk is conditioned on $\mathcal{K}$ (Knowledge). Then, the methodologies and approaches for risk assessment are to be seen as supports for incorporating knowledge in a systematic, rigorous and transparent framework. In other (simple and crude) words, risk assessment is a way of generating, representing and presenting the knowledge about the risk issues and their future occurrence, to allow taking decisions thereupon. This requires developing models based on the available knowledge, representing and expressing the related uncertainties, propagating the uncertainties and using proper metrics (probabilities or others) to describe risk. Such description of risk is inherently conditional on the knowledge $\mathcal{K}$.

The relatively recent discussions on the fundamental concept of "risk" and other foundational issues related to its assessment (Aven 2012a, 2012b, 2016a; Aven & Zio 2014; Cox 2015) have stressed and reinforced this common understanding that the outcomes of risk assessment are conditioned on the knowledge available on the system and/or process under analysis (Terje Aven, 2016b; Terje Aven & Zio, 2014; Zio, 2016c). Recognizing this, leads to accepting the inevitable existence of a residual risk related to the unknowns in the system, and/or process characteristics and behaviors.

Then, it is just as important to be aware of the (incomplete) knowledge conditioning the risk assessment outcomes, somewhat along the lines of thought of the former United State Secretary of Defense, Donald Rumsfeld, who said the following at the press briefing on 12 February 2002, addressing the absence of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups (Rumsfeld 2002):

"There are known knowns: things we know we know. We also know there are known unknowns: that is to say, we know there are some things we do not know. But there are also unknown unknowns: the ones we don't know we don't know."

Correspondingly, accident events and scenarios in a risk assessment model have been classified according to the knowledge available at the time of the assessment (Flage & Aven 2015):

1. Unknown-unknown
2. Unknown-known
3. Known-unknown
4. Known-known

In particular: 1) identifies those events and scenarios that were unknown to everyone, at the time of the risk assessment; 2) indicates those events and scenarios unknown to the risk analysts performing the assessment, but known to someone else; 3) identifies situations of awareness where the background knowledge is weak but there are indications or justified beliefs that a new, unknown type of event or scenario (new in the context of the activity posing the risk) could occur in the future; 4) indicates events and scenarios that are known to the analysts performing the risk assessment, and for which evidence exists.

According to (Flage & Aven 2015), events and scenarios belonging to 1-2 and 4, and associated to negligible probabilities of occurrence, are black swans in the sense of (Taleb 2007), whereas category 3 is representative of emerging risks, i.e., either new risks or known risks that, however, become apparent in new or unfamiliar conditions. Note that, clearly, the concepts of "new" and "known" are dependent on the background knowledge available.

For the sake of giving an example, consider the South Australia power network, which underwent a massive blackout caused by a cascading failure triggered by a heavy storm on the 28th Sep 2016. Around 1.7M people remained without power for 3h and some days were necessary to restore completely the energy supply. According to the preliminary report of the Australian Energy Market Operator (AEMO), the heavy storm was a "non-credible event", i.e., either an unknown-known or a known-known with a negligible probability associated. However, successive analyses have highlighted that the network had more vulnerabilities than expected and that many hazards were underestimated, e.g., those associated to wind and lightning: thus, a misuse or misinterpretation of knowledge available.

Yet, the issue of uncertainty and its interpretation remain difficult and somewhat controversial. In risk assessment it is arguable that everything is unknown to a degree and the classification of the accident events and scenarios in the four categories given above could be questionable. In particular, the first category (unknown – unknown) may be used in the realm of political sciences, where everything is debatable, but may be less acceptable/defensible in the context of formal and scientific, risk-informed decision making. It may be used to defend a decision after the fact, as in the case of the former United States Secretary of Defense. On the other hand, formal Decision Analysis recognizes the fact that a decision is made in the light of the existing knowledge (formalized by the risk assessment in the context here of interest). In this view, a decision maybe "right" in the sense that it is consistent with a given theoretical framework and a given body of knowledge but it might, after the fact, prove "wrong" (in terms of the actual outcome), because there is always a possibility of a bad outcome from a decision or because the body of knowledge is incomplete to allow taking the "right" decision. This is true also for any risk model, which is built and applied on the basis of the existing information and knowledge of the developer. Then, the degree of knowledge and information is something that indeed needs to be considered in risk assessment and management (Apostolakis, 2004).

From the above, we can retain that risk assessment amounts to a systematic and structured effort to organize the knowledge available on events, processes and scenarios that affect specific decisions to be made for the management of risk. For decision making, risk assessment must provide traceable information for arguing the decisions; the risk assessment outcomes must be communicated in a way that allow the decision makers to interpret them properly for their purposes and to understand the associated uncertainty related to the available knowledge used for the assessment. Risk assessment provides the framework for organizing the knowledge available on the system of interest, with the aim of understanding how the system can fail and prioritizing the failure modes so that good decisions can be taken (Flage & Aven 2015). The value of the solutions of risk assessment and of the management decisions that depend on them, then, stands on the quality of the methodologies and approaches that constitute the framework, and on the strength of the knowledge $\mathcal{K}$ which the framework incorporates. Whereas procedures of quality assurance have been developed for the former, it is still an open issue and a research challenge how to explicitly treat knowledge in risk assessment and management. How should it be described and evaluated in the risk assessment? How should it be reflected and taken into account in the decision-making process of risk management? The answers to these questions are critical for the validity of a risk assessment. When a risk assessment is performed to provide information that is used for making decisions, there must be a way to tell that it has been performed with adequate techniques and sufficient knowledge for making the decisions (Rae et al. 2012). Quality review of a risk assessment is essential, as opposition to a particular decision often takes the form of raising questions to the validity of the risk assessment (Apostolakis 2004).

3 Simulation for Risk Assessment

Overall, accidents and incidents can be considered as extreme states of behavior of the systems involved (Ale, 2016) and from the above said, it is clear that identifying and characterizing hazardous accident and event scenarios is a fundamental task of knowledge mining for risk assessment. This task is far from trivial in practice, given the complexity of the systems and processes: a large, combinatorial set of possible scenarios, events and conditions needs to be considered, of which only few, rare ones lead to critical, unsafe situations. This makes experimentation economically unsustainable and physically infeasible.

This is why simulation has long been advocated as a way to explore and understand system behavior for knowledge retrieval (Santner, Williams, & Notz 2003; Simpson, Poplinski, Koch, & Allen 2001), and has been used for safety assessment since the 1970s-80s. However, it is the continuous advancements in modelling techniques (including the fast-running artificial intelligence-based surrogate/meta-modelling) and the impressive increase in economical availability of computational power (including parallel computing and cloud computing) that are pushing to unprecented levels (and benefits) the use of simulation for exploring system behavior and advancing knowledge for risk assessment.

Within a simulation-based accident scenarios exploration, a set of simulations is run with different initial configurations of the system design and operation parameters (input), and the corresponding system state is computed (output). Evaluation of the system state with respect to specified safety conditions (critical thresholds) allows identifying the input configurations leading to critical system states. These states form the so called “Critical Regions” (CRs) or “Damage Domains” (DDs) (Montero-Mayorga, Queral, & Gonzalez-Cadelo 2014). The CRs may be identified corresponding to prior knowledge and expectation of the analysts or be “discovered”, i.e., the analysts are not a priori aware of such critical configurations and mining by simulation allows identifying them.

Concurrently, simulation can also be exploited to estimate the accident scenarios probabilities, or any other measure of uncertainty adopted to describe risk in (2)-(3). For this, Monte Carlo (MC) methods of stochastic discrete event simulation have been generally accepted as a gold standard (Labeau 1996; Marseguerra & Zio 1996; Kalos & Whitlock 2008; Dubi 2000; Zio 2013; Rubinstein & Kroese 2016). In practice, MC simulation consists in generating a large number of samples/trials/histories of system response and counting those that reach the state of interest, i.e. that end in the CRs (DDs). For example, for estimating the reliability of a system at a given time t, i.e., the probability that the system does not fail before *t*, a set of life histories of the system are run and the time at which the system fails (Time To Failure, TTF) in each history is recorded. Then, the reliability of the system at time *t* is estimated as the fraction of simulations whose TTF is larger than *t*. Likewise, estimating the probability of occurrence of an event leading the system into a given CR, defined by specific thresholds of system safety parameters (e.g. limit temperatures, pressures, heat fluxes etc.), can be done by sampling realizations of the system life and counting the fraction of times that the system ends in the CR of interest (Robert & Casella 2004).

Then, the two key research questions in the practice of risk assessment that can be addressed with the use of simulation models are:

- Identify hazardous conditions for the system, i.e., the pairs event-consequence $(\mathcal{A}, \mathcal{C}; \mathcal{K})$ in Eq. (3), which represent critical states of the system (i.e., identify the CRs of the system).
- Estimate the probability of occurrence of rare critical scenarios, i.e., $(\mathcal{Q}; \mathcal{K})$ in Eq. (3).

As simple and intuitive the use of simulation may seem for addressing the above two questions in the practice of risk assessment, it is actually quite demanding because the models of system behavior are:

- *High-dimensional*, i.e., with a large number of inputs and/or outputs;
- *Black box*, i.e., without an explicit Input/Output (I/O) relation (because coded in a computer program or because implicit in an empirical surrogate or meta-model, e.g. based on data and artificial intelligence);
- *Dynamic*, because the system evolves in time;
- *Computationally demanding* even for a sinlge trial simulation, as a consequence of the above characteristics of the models and of the numerical methods employed for their solution.

The high dimensionality in the inputs implies that the system conditions and scenarios to consider for simulating the system behavior for the identification of the CRs and/or for the estimation of the probability of their realizations (Au & Beck 2003a; Valdebenito, Pradlwarter, & Schuëller 2010), increase exponentially with the input space dimensions (Zio 2014). It also renders difficult the a posteriori scenario analysis for risk understanding, due to the difficulty of visualization of the results in such large spaces; this requires the development of specialized representation tools (Di Maio et al. 2011; Mandelli et al. 2013a; Maljovec et al. 2016; Liu et al. 2017).

Black box models, inevitably typically nonlinear, make it impossible to a priori identify the set of input configurations that lead the system into CRs. In practice, when the computational model is a black box (inherently because empirical, or because complicated even if physic-based), the only feasible way to do this is to run simulations and post-process the outcomes.

For dynamic systems, an additional dimension of complexity comes from having to deal with changes occurring to the system during its evolution in time, e.g., events that occur at different times (stochastically, e.g., components failures, or deterministically, e.g., control actions) and that affect the operation of the system (Siu 1994; Aldemir 2013; Mandellli et al. 2013b; Zio 2014; Mandelli et al. 2016; Ma et al. 2017a, b; Fan et al. 2017).

Although computational power is continuously increasing, in many practical instances computational cost still remains an issue for simulation-based risk assessment, because in such cases the high computational cost for the simulation of even a single system life history prevents the analyst from running and exploring the large number of input configurations for mining knowledge to characterize the system CRs. This is even more of an issue when analyzing highly reliable systems, i.e., systems characterized by very small probabilities of failure, whose CRs correspond to very small domains that are very hard to find in the large space of input configurations (Bucklew 2013; Rubino & Tuffin 2009).

Two main strategies are currently followed to address the two research questions and related challenges above presented:

- Simulation of large sets of system life histories using the increased computational power made available through parallel computing, cloud computing etc.;
- Simulation by adaptive sampling, which amounts to intelligently guiding the simulation towards the system states of interest (i.e., those belonging to the CRs). This entails that the simulation methods be capable of automatically understanding, during the simulation, which configurations are most promising to visit.

As answer to the first key research question formulated above, contributions are needed for the:

- Design and implementation of novel frameworks of adaptive simulation for discovering (unexpected) consequences associated to a known set of scenarios (Li et al. 2011; Turati, Pedroni, & Zio 2016a). Methods must be found to guide the simulations towards those scenarios that are more uncertain regarding the consequences they can lead to (i.e., those scenarios about which the knowledge $\mathcal{K}$ should be increased).
- Design and implementation of novel frameworks of adaptive simulation for the identification of CRs (Kleijnen 2009; Cerou and Guyader 2007; Echard et al. 2011; Munoz Zuniga et al. 2011; Cadini et al. 2014; Cadini et al. 2015; Turati, Pedroni, & Zio 2017). Benefitting from the advancements in modeling, artificial intelligence and machine learning, such frameworks can effectively combine model dimensionality reduction by feature selection/sensitivity analysis to screen important inputs, meta-modelling to reproduce the behavior of the computationally expensive model by a cheap-to-run one, efficient stochastic models for exploration of the system state space, non-supervised classification methods (i.e., clustering) and visualization techniques for high-dimensional spaces (e.g., Parallel Coordinates Plot; Inselberg 2007), to retrieve and represent the information of interest (i.e., the critical/safe regions).

As answer to the second key research question formulated above, effective algorithms are needed for the simulation of rare events in hybrid models, i.e., models where variables evolve according to physical laws that can change as a consequence of discrete (stochastic) events (M Villén-Altamirano & Villén-Altamirano 1991; van der Schaft and Schumacher 2000; Turati, Pedroni, & Zio 2016b).

Simulation of rare events in hybrid models has, indeed, become a fundamental issue in many applications. For example, the safety assessment of systems of autnomous cars using verification techniques entails ensuring safe trajectories from path planning of autonomous vehicles moving in dynamic environments (Lee and Peng 2005). In traffic scenarios, measurements, disturbances and decisions of traffic participants are uncertain. This leads to a set of possible initial states, disturbance trajectories and behavior predictions for each road actor, with a potentially infinite number of reachabe outcome states of a traffic scenario over a given time horizon. As one cannot simulate all possible behaviors of traffic actors, effective simulation techniques for hybrid model verification are needed to probe the (rare) events of interest, i.e., typically those potentially leading to accidents (Botchkarev and Tripakis 2000; Tomlin et al. 2003). Based on the reachable states of an autonomous car and other actors in the surrounding, a probability of crash can be obtained (Althoff et al 2007).

Simulation is also strongly advocated for the hazard analysis, and safety and resilient assessment of critical infrastructures and systems of systems (Alexander & Kelly 2013; Zio 2016). The increasing concern on the vulnerability of critical infrastructures (see Section 5 below) and the increasing role of systems of systems in safety-critical applications has raised the need for methods to analyse their hazards, and verify their safety and resilience properties. One viable way for this is simulation of the variety of scenarios that can emerge from the response of the individual system components to different perturbations and failures, sampled over space and time. The effects of the interaction between system components can, then, be observed together with the corresponding system behaviour that emerges. The challenges for the analysis of such systems come from the fact that the system boundary is not well defined and the set of components in the system can vary over time, either as part of normal operation (e.g. a new car enters the traffic scene or a new aircraft enters a controlled airspace region) or as part of evolutionary development of the system itself (a traffic lane is interrupted because of construction work or a military unit receives a new air-defence system). In such an undefined and dynamic setting, conventional techniques of analysis may be inadequate for determining whether or not the failure of a given component may be hazardous for the system as a whole. Simulation, on the other hand, can provide a way of analysis of such systems made of multiple components that interact in complex and continually changing ways.

4 Extended Risk Assessment: business continuity and resilience

As mentioned in the Introduction, systems are increasingly exposed to hazards of disruptive events (Zio 2016), e.g., unexpected system failures (Hameed et al. 2016), climate change and natural disasters (Meng et al. 2015, Yang 2014, Yamaguchi et al., 2017), terrorist attacks (Reniers and Audenaert 2014). Risk assessment is, then, applied to inform risk management on how to protect from the potential losses caused by the disruptive events (Aven and Cox 2016; Zio, 2016; Yang et al. 2015, Zhang et al., 2014). As for the risk description (3), the focus is on the accident scenarios, their possible consequences and likelihoods, and the uncertainties therein (Bjerga and Aven 2016). The post-accident recovery process, is not considered.

Yet, given that the sources of hazard leading to disruptive events are extremely uncertain and, thus, difficult to describe and model quantitatively, and that the systems are highly connected to each other so that the impact of the disruption extends beyond the boundary of the individual systems, an extension of the framework of assessment is necessary, for an integrated management of risk and coherent use of the available resources. The framework must incorporate aspects beyond those of prevention, typical of risk assessment, in order to allow accounting for:

- the fact that the potential losses suffered from a disruptive event also depend on the after-the-fact recovery process;
- the recognition of the new World that digitalization has brought, with the new systems and services that are emerging. For example, according to a survey by IBM Global Services (Costs 2016), in 2008, enterprises in IT sectors have been estimated to suffer from an average revenue cost of 2.8 million US dollars per hour for unplanned application outages inefficiently recovered. Another report reveals that for a company that operates data centers, the average downtime cost per minute has exceeded $5000 (Downtime 2016). An extension of the conventional risk assessment and management methods is, then, needed, so that the recovery process can be integrated.

Efforts in this direction have been made, particularly in the areas of socio-technical systems (Leger et al., 2008) and occupational risk. As an example of a working model in which causes, effects and remedial actions are integrated can be found in (Papazoglou et Ale, 2007), with the treatment of the uncertainties in and by that model as in (Papazoglou et al., 2015). Implementation of a model for a complex socio-technical system can be found in (Ale et al., 2009).

To proceed further into the reflections on the need and challenge of extending the framework of risk assessment to cover the pre- and post-accident scenarios analysis, the affine concepts and paradigms of business continuity and resilience are discussed from the perspective of their links to system reliability/availability and safety.

4.1 Business continuity

Business continuity (BC) is defined as "the capability of an organization to continue delivery of products or services at acceptable levels following disruptive events" (ISO, 2012). It measures the capability of an organization to remain at or quickly recover to operational states after being affected by disruptive events. Business Continuity management (BCM) is a managerial framework that aims at ensuring that no disruptive events can lead to unexpected, unwanted interruptions of production or service activity. In this view, it lays down the vision of integrating the post-accident recovery process to the preventive view of risk assessment (Cerullo and Cerullo, 2004). Indeed, such framework of BCM is defined by the International Organization of Standards (ISO) as "an holistic management process that identifies the potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities" (ISO, 2012). From this definition, it is clear the reliability/availability perspective and the link with the resilience concept also in a safety perspective.

As an integrated management strategy aiming at reducing the technological and operational risks that threaten the recovery from disruptions and interruptions, BCM has attracted quite some attention in the last couple of decades (Herbane, 2010). A comprehensive approach to BCM planning is proposed in (Cerullo and Cerullo, 2004), with particular focus on internal and external information security threats. The necessity and benefit of implementing BCM in an organization is discussed in (Zsidisin et al., 2005). The application of BCM planning to achieve organizational disaster preparedness at Boeing is surveyed in (Castillo, 2005). An integrated framework to support BCM planning is presented in (Gibb and Buchanan, 2006). The historical evolution of BCM is reviewed in (Herbane, 2010), with the critical events that motivated its development. In (Snedaker, 2013), BCM is compared to the conventional risk management methods and the comparison clearly shows that BCM not only focuses on the protection of the system before the crisis, but also on the recovery process during and after the crisis. A model to assess the maturity of the BCM programs is developed in (Randeree et al., 2012) and applied on a case study from United Arab Emirates (UAE) banking sector. System reliability models to plan BCM are used in (Faertes, 2015). A framework to integrate BCM and disaster recovery planning, to ensure that the system would resume and recover its operation in an efficient and effective way is presented in (Sahebjamnia et al., 2015). Methods to ensure the business continuity of a safety-related power supply system are presented in (Parise et al., 2016). An enhanced risk assessment framework to support business continuity management is developed in (Torabi et al., 2016). A fuzzy cost-benefit analysis method for planning BCM strategies is presented in (Rabbani et al., 2016).

As a holistic, integrated risk management strategy, BCM offers great potential benefits but the complexity of the systems and risk problems involved is such that most currently existing BCM strategies are based on qualitative methods only, and this limits practical and effective application. Very few works concern the quantitative modeling and analysis of BC. An approach to model the system behavior in the BC process, based on process algebra and modal logic, has been presented by (Boehmer et al., 2009). Similar models have been applied in (Brandt et al., 2009) to describe the BC process of a credit card company. A multi-layer model is developed in (Asnar and Giorgini, 2008) to model the BC of a loan originating process. In (Bonafede et al., 2007), Cox's model and Bayesian networks are combined to model the BC process. A simulation model is developed in (Tan and Takakuwa, 2011) to investigate the BC of a company considering the outbreak of a pandemic disease, where the BC is characterized by the operation rate and the plant-utilization rate. These models describe the post-crisis behavior of the system. However, no clearly defined business metrics have been proposed from these models, which impedes the quantitative analysis of BC and, therefore, limits application in practice.

To contribute to the advancement of BCM for its application in practice, (Zeng and Zio, 2017) have developed an integrated, quantitative framework for modeling BC, founded on the definition of four metrics that measure the potential losses caused by the disruptive events. A simulation-based method has been presented in the paper to calculate the BC metrics based on the integrated model. To demonstrate the use of the framework, the BC of an oil storage tank farm is assessed. The conceptual model that describes BC and identifies its major contributing factors refers to a performance indicator, denoted by PPIB (Process Performance Indicator-Business), whose value reflects the degree to which the objective of the system is satisfied. For example, for an oil refinery, the PPIB is its daily production yield; for a manufacturing factory, the PPIB is the products produced per day. The values of PPIB are determined by the operation state of the system: the PPIB remains at its nominal value when the system is under normal operation and drops to a degraded value when the normal operation of the system is disrupted. In practice, an organization is susceptible to various disruptive events, which might jeopardize its BC. As already mentioned, commonly encountered disruptive events include:

- technological disruptions, caused by components or systems failures;
- natural disruptions, caused by natural disasters, e.g., floods, earthquakes, lightning, etc.;
- social disruptions, caused by social movements, e.g., terrorist attacks, strikes, supply chain disruptions, etc.

When one or some of these disruptive events occur, the normal operation is disrupted and PPIB drops to a degraded value, because of the disruptive events. The production stakeholders, then, suffer from losses caused by the business interruption. To reduce such losses, various BC measures can be taken to guarantee the continuity of the business process. Generally speaking, those measures can be divided into four categories, i.e.,

- protection measures, for defending the system from the disruptive events and preventing them from damaging the system. If protection measures succeed, the business process is not interrupted;
- mitigation measures, which intervene when the protection measures fail and initial damage has been caused by the disruptive events. The aim of the mitigation measures is to contain the evolution of the disruptive events at the early stages of development, so that damages can be mitigated;
- emergency measures, which must come into play when the mitigation measures fail to contain the damage, and often require significant human intervention;
- recovery measures, which aim at re-establishing normal operation, ex-post.

For example, lightning is a severe threat to oil & gas systems (Chang and Lin 2006). Often, a lightning protection mast is installed at oil and gas tank farms as a protection measure against the threat of lightning (Necci et al. 2014). If the protection mast fails to protect the system, the oil storage tank might catch fire (Necci et al. 2013). Mitigation measures, such as the automatic fire extinguishing system, are automatically activated to fight the fire in order to prevent it from spreading to other tanks, causing a domino effect (Necci et al. 2013). Emergency measures, e.g., the intervention of a fire brigade, are needed when the mitigation measures fail to stop the propagation of the accident (Wu and Chen 2016). Then, recovery measures, e.g., the repair and restoration of the affected tanks, are carried out to recover operation and minimize the losses caused by the business interruption.

Fig. 1 presents the conceptual model that schematically illustrates the evolution of a business process under a disruptive event (Zeng and Zio 2017). The business process is divided into four phases:

protection, mitigation, emergency and recovery. Each phase is associated with the corresponding business continuity measure. As shown in Fig. 1, the PPIB of an actual business process might deviate from its nominal value due to the presence of various disruptive events. The severity and duration of the business interruption caused by the disruptive event can be controlled by implementing business continuity measures in the different phases. Among them: protection measures affect the resistance of the system to disruptive events; mitigation and emergency measures determine how much system performance is degraded from the damage caused by the disruptive event; recovery measures influence how quickly the system can recover its performance to normal operation.

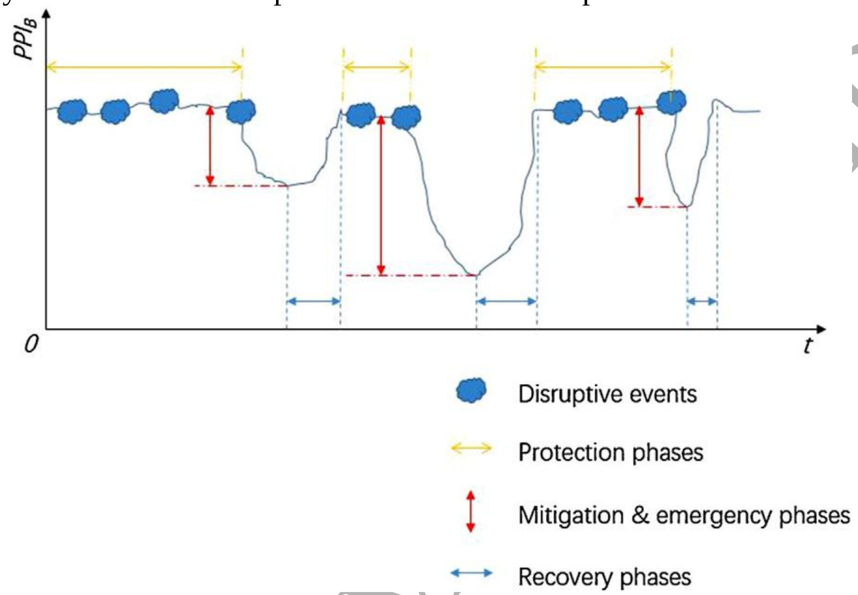

Fig. 1 – A conceptual model for the business continuity process. (Zeng and Zio 2017)

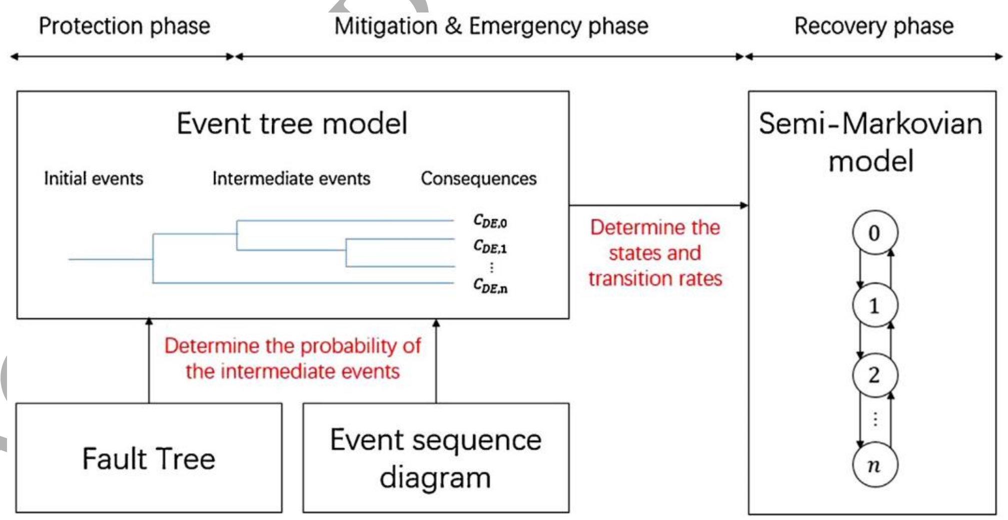

Fig. 2 – An integrated model for business continuity assessment. (Zeng and Zio 2017)

As shown in Fig.1, the business process comprises of the protection, mitigation, emergency and recovery phases. Since each phase has its own characteristics, different modelling approaches need to be integrated to capture the phase-specific characteristics. An example of integrated modeling framework is presented in Fig. 2 (Zeng and Zio 2017). The protection, mitigation and emergency phases determine the consequences of the disruptive event. Event trees can be used to model these phases (Zio 2007). In an event tree model, the probabilities of the intermediate events represent the reliabilities/uncertainties of the allocated business continuity measures. The outcomes of the protection and mitigation phases depend on the reliabilities of the protection and mitigation measures, respectively. Fault tree models can be used to calculate these intermediate probabilities (Zio 2007). The result of the emergency phase, on the other hand, involves the modeling of a sequence of activities by the emergency response team. Models capable of considering the sequential dynamics of such activities should be used for the emergency phase, e.g., the event sequence diagram (Zhou et al. 2016). The recovery process also involves the dynamics of maintenance actions, which can be effectively described in terms of the process of transitions between system states, e.g., by semi-Markovian models (Compare et al. 2016).

4.2 Resilience

Resilience is a concept closely related to BC. Here, its consideration is given particularly in relation to accidents and, thus, to its specificity with respect to safety, rather than reliability and availability of production, or other attributes of functionality for systems and critical infrastructures (CIs).

As mentioned earlier, risk-based approaches have been used to assess hazards and mitigate consequences associated with their impact. By identifying the components contribution to the overall system risk, the outcomes of risk assessment enable prioritized decisions for system improvements to buy down risk. But as already said, the rapid technological evolution, combined with the unprecedented uncertain nature and extent of emerging hazards, makes it difficult to characterize all potential hazards and estimate accurate probabilities of occurrence and magnitude of consequences, that decision makers can confidently rely on for their risk-reducing decisions. This is particularly true for the complex, interconnected systems that make up today's critical infrastructures and calls for the extension of the framework of risk assessment and management, to make these systems resilient to the wide range of hazards within specific cost and time restraints, and considering the large uncertainties. Differently from the concept of risk, resilience is focused also on the ability to prepare and recover quickly from an accident or disruptive event, which may be known or unknown. Managing for resilience, then, requires ensuring a system's ability to plan and prepare for the potential occurrence of accidents and disruptive events, and then absorb, recover, and adapt in case of occurrence.

It is the lessons learned in recent years from some catastrophic accidents that have led to the concept of resilience to ensure the ability of systems and CIs to withstand, adapt to and rapidly recover from the effects of a disruptive event (Moteff 2012; Obama 2013; Pursiainen 2009). The outcomes of the 2005 World Conference on Disaster Reduction (WCDR) confirmed the significance of the entrance of the term resilience into the disaster discourse and gave birth to a new culture of disaster response (Cimellaro et al. 2010). As a result, today's systems are not only required to be reliable but must also be able to recover from disruptions (Zio 2009, Zio 2016b). Government policy has also evolved to encourage efforts that would allow assets to continue operating at some level, or quickly return to full operation after the occurrence of disruptive events (Moteff 2012). Consequently, resilience is nowadays considered a fundamental attribute for systems and CIs that should be guaranteed by design, operation and management.

The concept of resilience varies somewhat by discipline and application (Najjar and Gaudiot 1990; Henry and Ramirez-Marquez 2012; Ouyang et al. 2012; Uday and Mareis 2015), and different definitions exist such as "the ability of the system to reduce the chances of shock, to absorb a shock if it occurs and to recover quickly after a shock (re-establish normal performance)" (Bruneau et al. 2003), "the capacity of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident" (U.S. Department of Homeland Security 2009), the "ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks" (Haimes 2009). From these definitions, it emerges that resilience is characterized in terms of four properties, i.e. robustness, redundancy, resourcefulness, rapidity and four interrelated dimensions, i.e., technical, organizational, social, economic. It can be considered a new paradigm for risk engineering, which proactively integrates the accident preventive tasks of anticipation (imagining what to expect) and monitoring (knowing what to look for), the in-accident tasks of responding (knowing what to do and being capable of doing it) and learning (knowing what has happened), the mitigative tasks of absorbing (damping the negative impact of the adverse effect) and the recovery tasks of adaptation (making intentional adjustment to come through a disruption), restoration (returning to the normal state) (Hollnagel et al. 2006).

Various models, methods and frameworks for analyzing and quantifying resilience have been proposed in the literature (Carpenter et al. 2001; Fiksel 2003; Wreathall 2006; Jackson 2007, 2009; Peters et al. 2008; Madni and Jackson 2009), with focus on diverse fields of application such as seismic engineering and structural systems (Cimellaro et al. 2006; 2010; Poljanfisek et al. 2012; Duenas-Osorio and Kwasinski 2012), ecological systems (Holling 1973), economics and financial systems (Starr et al. 2003; Rose et al. 2009; Amini et al. 2013; Baroud et al. 2015), service systems (Todini 2000; Rosenkrantz et al. 2009), telecommunication systems (Omer et al. 2009), urban infrastructures (Jin et al. 2014; Oyuang and Duenas-Osorio 2012; Attoh-Okine et al. 2009), disaster analysis for avoidance and recovery (Bonanno et al. 2007; Tierney and Bruneau 2007; Zobel 2011)

While resilience can be characterized by many system features and attributes, recovery is a vital element of strategies to improve resilience. System recovery and its role in infrastructure system resilience have attracted quite some attention. Some studies have modelled the post-disaster restoration of various infrastructure systems in an effort to estimate the expected restoration time (Ferrario and Zio 2014; Liu et al. 2007; Shinozuka et al. 2004), and several others have compared the performance of different restoration strategies (Buzna et al. 2007; Çağnan et al. 2006). Other works have tackled the problem of post-disaster restoration strategy planning and optimization, for the purpose of restoring system service in a timely and efficient manner. Considering multiple types of systems simultaneously, (Kozin and Zhou 1990) developed a Markov process to describe the process of infrastructure system recovery; then, they used dynamic programming to estimate the repair resources required for each time step and for each system, so as to maximize the expected economic return from system functioning. In (Noda 1993), a neural network was used to minimize the likelihood of post-earthquake functional loss for a telephone system. A mixed- integer programming approach was applied in (Bryson et al. 2002) for selecting a set of recovery subplans giving the greatest benefit to business operation. Restoration when multiple infrastructures, operated by different firms, are involved was addressed in (Casari and Wilkie 2005). A case of network restoration was addressed in (Lee et al. 2007), involving the selection of the location of temporary arcs (e.g., shunts) needed to completely re-establish network services over a set of interdependent networks: a mixed-integer optimization model was proposed to minimize the operating costs involved in temporary emergency restoration. A genetic algorithm was applied in (Xu et al. 2007) to optimize the restoration of electric power after an earthquake: the objective of the optimization was the minimization of the average time that each customer stays without power. An integer programming model was proposed in (Matisziw et al. 2010) to restore networks where the connectivity between pairs of nodes is the driving performance metric associated with the network. The studies cited above involving the optimization of post-disaster CI restoration apply a variety of modelling approaches and focus on different aspects of the restoration strategy (e.g. the repair order of damaged components, where and how to allocate repair resources, and so on).

In more general terms, the resilience analysis of complex systems and CIs cannot be carried out only with classical methods of system decomposition and logic analysis. Furthermore, large uncertainties exist in the characterization of the failure behavior of the elements of a complex system, of their interconnections and interactions (Zio and Aven 2011). A framework is, thus, needed to integrate a number of methods capable of viewing the complexity problem from different perspectives (topological and functional, static and dynamic), under the existing uncertainties (Ouyang et al. 2009; Reed et al. 2009; Kröger and Zio 2011; Ouyang 2014):

- structural/topological methods based on system analysis, graph theory, statistical physics, etc.; these methods are capable of describing the connectivity of a complex system and analyzing its effects on the system functionality, on the cascade propagation of a failure and on its recovery (resilience), as well as identifying the elements of the system which must be most robustly controlled because of their central role in the system connectivity (Newman et al. 2005; Lee et al. 2007; Zio and Sansavini 2011; Fang and Zio 2013; Alipour et al. 2014; Kahkzad and Reniers 2015; Praks et al. 2015);
- logical methods based on system analysis, hierarchical logic trees, game theory, etc.; these methods are capable of capturing the logic of the functioning/dysfunctioning of a complex system due to random effects and malicious attacks, and of identifying the combinations of failures of elements (hardware, software and human) which lead to the loss of the system function (Apostolakis and Lemon 2005; Bobbio et al. 2010; Kahkzad 2015; Zhang et al. 2015);
- phenomenological/functional methods, based on transfer functions, state dynamic modeling, input-output modeling and control theory, agent-based modeling etc.; these methods are capable of capturing the dynamics of interrelated operation between elements (hardware, software and human) of a complex system and with the environment, from which the dynamic operation of the system itself emerges (Trucco et al. 2012; Alessandri and Filippini 2013);
- flow methods, based on detailed, mechanistic models (and computer codes) of the processes occurring in the system; these methods are capable of describing the physics of system operation, its monitoring and control (Sansavini et al. 2014).

The integration of these methods is expected to enable capturing the different relevant aspects of the complex systems (Deng et al. 2015). For electric power grids, for example, comparisons between structural/topological and power flow methods have been made. Some studies (Baldick et al. 2008; LaRocca et al. 2015; Sun and Han 2005; Correa et al. 2013) have provided qualitative comparisons between complex network theory models and power flow models, identifying similarities and differences, and evaluating advantages and disadvantages. Also, by extensive comparative simulation, (Cupac et al. 2013) has shown that a network-centric model exhibits ensemble properties which are consistent with the more realistic optimal power flow model. Most recently, (Matisziw et al. 2010) conclude on the appropriateness of graph theory techniques for the assessment of electric network vulnerability by comparison to physical power flow models. This is confirmed in (Fang et al. 2014), where the problem of searching for the most favorable pattern of link capacities allocation that makes a power transmission network resilient to cascading failures with limited investment costs is formulated within a combinatorial multi-objective optimization framework and tackled by evolutionary algorithms. Two different models of increasing complexity are used to simulate cascading failures and to quantify resilience: a complex network model, and a more detailed and computationally demanding power flow model. Both models are tested and compared on a case study involving the 400kV French power transmission network. The results show that the optimal solutions obtained using the two different models exhibit consistent characteristics in terms of phase transitions in the Pareto fronts and link capacity allocation patterns.

5 Dynamic Risk Assessment and Condition Monitoring-Based Risk Assessment

Risk assessment must account for the time-dependent variations of components and systems, as they operate, age, fail, are repaired and replaced (Villa et al. 2016). For this, updates are performed to reflect the components and systems changes and the corresponding current overall system/plant safety state, leading to what is called Living PRA (LPRA). LPRA is a system/plant specific PRA that can be updated or modified, when necessary, to reflect the system/plant changes during its lifetime (Johanson and Holmberg 1994). Changes can be physical (resulting from plant modifications, etc.), operational (resulting from enhanced procedures, etc.), organizational, but also changes in knowledge due to the acquisition of operational experience, field data, etc. The updated LPRA, then, reflects the current design and operational state of the system/plant, and is documented in a way that each aspect of the model can be directly related to existing system/plant information, documentation or analysts assumption (Lin et al. 2015).

Extending the concept of LPRA, Dynamic Risk Assessment (DRA) is defined as a risk assessment that updates the estimation of the risk of a deteriorating system according to the states of its components, as knowledge on them is acquired in time (Khan et al. 2016; Yadav et al. 2017). DRA is capable of capturing the time-dependent behaviour of the system risk profile (Khan et al. 2015, 2016; Villa et al. 2016; Heo, 2016).

An early attempt of DRA was conducted in (Meel and Seider 2006, 2008) where Bayes theorem was used to dynamically update the estimates of accident probabilities, using near misses and incident data collected from similar systems. A similar DRA method was developed in (Kalantarnia et al. 2009), where Bayes theorem is used for probability updating and Event Tree (ET) analysis is used for consequence modeling. ET was used in (Roy et al. 2015) to model the accident sequences of an ammonia storage unit and Bayes theorem for DRA. ET and Bayes theorem were used in (Pariyani et al. 2012) to update the risk in chemical process industries based on data from a large near-miss data base. A hierarchical Bayesian model for DRA was developed in (Khakzad et al. 2014) and applied to analyze the near-accident data of offshore blowouts. A similar hierarchical Bayesian model was used in (Yang et al. 2013) to dynamically assess the risk of an offshore drilling platform.

In (Khakzad et al. 2012), Bayes theorem was combined with a Bow-Tie (BT) model for DRA: failure probabilities of the primary events and safety barriers in the BT were constantly revised over time and the updated BT model was used to estimate the updated risk profile. BT was used in (Paltrinieri et al. 2014) to support the DRA from metal dust accidents. (A similar method was applied in Abimbola et al. 2014) to update in real time the risk estimation of offshore drilling operations. A DRA method using a Bayesian Network (BN) model was developed in (Khakzad et al. 2013), where the probabilities of the basic events in the BN are updated when new accident data are collected. A comparison of the BT-based and BN-based methods were made in (Khakzad et al. 2013b), and a procedure was given to map a BT into a BN. The DRA for assessing the risk from leakage failure of submarine oil and gas pipelines was addressed in (Li et al. 2016) using BT and BN. In (Zarei et al. 2017), BN was applied for the DRA of a natural gas station.

Most existing DRA methods, as reviewed above, only use statistical data, i.e., count data of accidents or near misses from similar systems, to update the estimated risk indexes. It should be noted that in some literature, these statistical data are also called Accident Sequence Precursor (ASP) data

(Meel and Seider 2008, 2016; Kalantarnia 2009). A drawback of using only statistical data is that one must wait until accidents or near misses (precursors) occur before updating the estimation of the risk indexes. Besides, statistical data are collected from similar systems, reflecting population characteristics but not fully accounting for the individual features of the target system.

Additional information potentially useful for the estimation of the risk indexes may come from condition-monitoring data. In practice, accident initiating events and safety barriers failures usually occur as a result of degradation mechanisms, e.g., wear (Zeng et al. 2016), corrosion (Zeng et al. 2014), fatigue (Jiang et al. 2016), crack growth (Baraldi et al. 2012), oxidation (Compare et al. 2016), etc. The degradation processes can be monitored in real time and failures can be predicted and anticipated with reference to specific thresholds of the monitored variables. The condition-monitoring data give information on the individual degradation process of the target system and of the safety barriers, and provide the opportunity to update the reliability values before actual failures occur. Therefore, introducing condition-monitoring data in DRA could be a beneficial complement to the statistical data, towards a condition monitoring-based risk assessment (CMBRA).

In this direction, a few initial attempts of using condition-monitoring data in DRA have been made. Kalman filtering has been applied in (Zadakbar et al. 2013) to estimate the true degradation states from condition-monitoring data and DRA (or CMBRA) based on a loss function associated with the degradation states has been conducted. Similar works were also conducted by the same authors using different condition-monitoring techniques, i.e., Particle Filtering (PF) (Zadakbar et al. 2015) and Principal Component Analysis (PCA) (Zadakbar et al. 2012). To deal with nonlinear and non-Gaussian features, (Yu et al. 2014) developed a self-organizing map-based approach for CMBRA using condition-monitoring data. The concept of remaining time was proposed by (Wang et al. 2016) and used to develop a CMBRA method for multiple condition-monitoring variables. A CMBRA by monitoring sensitive variables of a passive residual heat removal system, but without considering the possible noise in the monitored data, was conducted by (Kim et al. 2015). However, these existing methods consider only the condition-monitoring data, but no statistical failure data. Besides, most of the existing methods do not involve consequence analysis models, e.g., ET, BT, BN, etc., when calculating the risk indexes. Rather, the risk indexes are assessed directly from the monitored degradation variables by considering the affected performance due to the degradation.

A method for DRA that allows the joint utilization of statistical and condition-monitoring data has been proposed in (Zeng and Zio 2017b). Consequence analysis is also considered by means of an ET. A first step in the DRA is to online update the reliability of the safety barriers using the two types of data. For this, a hierarchical Bayesian reliability model is developed. Based on the model, an online assessment algorithm is developed for the reliability values. Statistical data refer to the count data of the consequences of accidents that occur during the operation of similar systems, thus providing “population” information, while condition-monitoring data come from online monitoring the degradation of the specific target system of interest and describe system-specific features.

6 Safety and Security of Cyber-Physical Systems

With the large development of digitalization in the industrial world, nowadays, CPSs are applied in many technological areas, including aerospace, automotive, energy, chemical industry, materials, civil transportation, agriculture and healthcare. A CPS features a tight combination of (and coordination between) the system computational units and physical elements. To the benefit of safe operation, the integration of computational resources into physical processes is aimed at adding new capabilities to stand-alone physical systems, to enable functionalities of real-time monitoring, dynamic control and decision support during normal operation as well as in case of accidents. For self-adaptive properties and extensive capabilities of autonomous "decision making" and handling of uncertain operational scenarios, CPSs rely on control systems that utilize software intensive model-based paradigms. When compared with more traditional system design frameworks, model-based developments undoubtedly provide greater capability and flexibility to rapidly define, analyze and integrate different aspects of a given design. However, this expanded capability and flexibility, and the dynamic nature of the model-based design environment, also pose challenges to the execution of traditional design validation and verification (V&V) processes. It is, thus, essential that methods and tools be made available also to facilitate the task of demonstrating compliance of control systems developed in such a model-based environments with safety-related requirements and any applicable certification standard (Guarro et al., 2017).

In CPSs, cyber and physical processes are dependent and interact with each other through feedback control loops (e.g., embedded cyber controllers monitor and control the system physical variables, whilst physical processes affect, at the same time, the monitoring system and the computation units by wired or wireless networks (Kim and Kumar, 2012; Lee, 2008; Alur, 2015)). The benefit of such self-adaptive capabilities is the reason why CPSs are increasingly operated in energy, transportation, medical and healthcare, and other applications (Lee, 2008; Khaitan and McCalley, 2015; Bradley and Atkins, 2015).

In the context of CPSs, sensor measurements can be used to monitor the behavior of the systems under different operational conditions, including hazardous and malicious ones. Indeed, CPS functionality and integrity can be compromised by both hazards (safety related) and malicious threats (security related) (Piètre-Cambacédès and Bouissou, 2013; Kriaa et al., 2015; Zalewski et al., 2016). Hazards and cyber threats originate from different sources (stochastic degradations and accidental conditions, for the former, external malevolent activities that are usually less accessible and less predictable for the latter (Aven, 2009; Kriaa et al., 2015)). Distinct properties and mechanisms between them suggest different assessment methodologies for their identification.

CPSs demand that in the risk analysis both safety and security aspects be considered (Eames and Moffett, 1999; Kriaa et al., 2015; Piètre-Cambacédès and Bouissou, 2013; Zalewski et al., 2016). With respect to safety, hazards relate to components failures that can result in accidental scenarios leading to unacceptable consequences on the system physical processes; as for security, malicious attacks can impair both the physical and cyber parts of the system, possibly leading to unacceptable consequences.

Failures of both hardware and software can compromise CPS integrity and functionality (NASA, 2013). During operation, failures of embedded hardware components (e.g., sensors and actuators) can be induced by aging, degradation, and process and operational conditions, which modify the way components work and interact with each other, generating multiple failure modes (Wang et al., 2016b). For example, sensors can degrade and fail in different modes such as bias, drift and freezing (Wang et al., 2016b); actuators can fail stuck, accidentally driving the physical process to be isolated from the controlling units of the cyber domain (Zio and Di Maio, 2009; Zaytoon and Lafortune, 2013).

Components failures can lead to two types of misoperations: (1) failure on-demand, e.g., failing to trigger protections or execute proper control strategies (when demanded); (2) malfunction, e.g., spurious triggering of protections (e.g., unintentional shutdown) or incorrect execution of control actions. Failures on-demand and malfunctions of both hardware and software components have gained increasing attention in the risk community (Aldemir et al., 2010; McNelles et al., 2016).

Resilience of CPS to failures can be granted by self-adaptiveness of control decisions on actuators, resorting to intelligent control systems that properly manipulate sensors measurements (Machado et al., 2016). For example, Proportional-Integral-Derivative (PID) controllers, typically used as feedback controller in CPS to retroact to actuators the actions to be undertaken for responding to changes of physical parameters, may suffer of software failures/errors (generated from inadequate specification, incomplete testing scope and algorithm/logic failures) that are latent and triggered only when context modifications are to be met (Aldemir et al., 2010; Jockenhövel-Barttfeld et al., 2016). In these situations, control rules adaptability to variable physical conditions is a fundamental requirement to the robustness of CPS for resilience during CPS operation.

CPSs reliance on digitalization and remote control systems increases their exposure to cyber attacks to controllers, databases, networks and human-system interfaces, that can result in the loss of system integrity and/or functionality. Malicious activities can be manifested as Denial of Service (DoS) attacks (Zargar et al., 2013; Yuan et al., 2013; Rahman et al., 2016), False Data Injection (FDI) attacks (e.g., packet/data modification) (Liang et al., 2017; Tan et al., 2017; Mohammadpourfard et al., 2017), network scan & sniffing attacks (Trabelsi and Rahmani, 2005; Rahman et al., 2016), integrity attacks (e.g., through malware contagion) (Ntalampiras, 2015; Ntalampiras, 2016) and, illegal command executions (Shin et al., 2015). They can be initiated in the cyber domain through local or remote accesses, mimicking the components failures but isolating the connectivity between cyber and physical systems, leaving the physical process uncontrolled and possibly drifting towards severe consequences.

Cyber attacks can cause serious security and privacy issues (Xiang et al., 2017). Under cyber attacks, e.g., by contagion of malware, security-related system features may result to be compromised and, the system safety and security potentially endangered. The identification of the cyber threats most affecting the system response is quite important for decision-making on optimal protection and resilience, as prevention and mitigation of malicious attacks contribute to guaranteeing CPS integrity and functionality (Yuan et al., 2014; Fang and Sansavini, 2017; Hu et al., 2017; Wang et al., 2017).

From the perspective of integrated safety and security of CPSs, distinguishing cyber attacks from component failures is important for evaluating the potential impacts on the system integrity and defining proper protection and mitigation actions for resilience. To make CPSs resilient, it is necessary to integrate the knowledge on cyber security, human interactions and complex networks, to address all possible failure and threats in a comprehensive and holistic way. For this, frameworks are still needed.

7 Conclusions

Risk assessment is a mature discipline, widely applied in practice for the design and operation of safe systems. The assessment involves a structured analysis of the system of interest to qualitatively and quantitatively describe risk, based on the available knowledge. The quantitative analysis is often criticized in view of the difficulty of assigning probabilities (e.g., to human errors or software failures), the difficulty of verifying the assumptions behind the models at the basis of the assessment, the inherent uncertainty involved in the phenomena of interest. However, the use of quantitative measures remains essential for rational, effective decision making combining evidential knowledge and subjective beliefs. The decisions that need to be made will be better if quantitative (and peer reviewed) information is available. For this, we need to provide risk outcomes that are either certain (a given accident scenario would indeed definitely occur) or of quantified uncertainty (there is a given probability that the accident may occur), and can, thus, be compared for risk prioritization and resource allocation. By engaging in quantifying the uncertainties and identifying the risk contributors, risk assessment contributes to the understanding of the risk and provides information useful for its regulation and management. For this, the quantitative measures must express how much, to what degree, we know about the event and, thus, how much we believe in its assessment. In this sense, they are an argument tool in support of the decision making. It is the duty of the risk analysts to make transparent the way the quantitative measures have been calculated. The risk assessment must, thus, provide an argument that it must be possible to scrutinize and not a formalized demonstration of an objective truth. The argument stands on the knowledge available and the related modeling assumptions made to formalize the assessment.

In this view, the increasing modeling and computational capabilities and data availability open great opportunities for mining knowledge and improving models for use in risk assessment. In this respect, we have discussed and analyzed some research and development directions with regards to the use of simulation for accident scenario identification and exploration, and the reliance on data for condition monitoring-based, dynamic risk assessment.

As for simulation, although it has long been thought has a fundamental asset for the future development of risk assessment, it is the advancement in modelling and computing capabilities that is nowadays making it actually feasible. Yet, for taking full deployment of simulation, and for taking the related benefits, trust must be put in the fast-running artificial intelligence-based techniques of surrogate/meta-modelling for their controlled application in exploring system behavior and risk assessment, with adequate treatment of the errors and uncertainties introduced by the associated approximations.

Regarding condition monitoring-based, dynamic risk assessment, the increased availability of sensors-monitored condition data is indeed opening new horizons to develop conditon-informed risk assessment that can be more representative of the actual state of the components and systems. There, frameworks of integration of the condition data-driven predictive models into the risk assessment model must be soundly developed and practically implemented, for actual industrial benefit.

The changes and innovations that the World is experiencing, with digitalization and the complexity of cyber-phyiscal systems (CPSs), climate change and extreme natural events, terrorist and malevolent threats, challenge the existing methods to describe and model quantitatively risk. In this respect, we have discussed and analyzed some research and development directions with regards to the extension of risk assessment into the framework of resilience and business continuity, and the safety and security assessment of CPSs.

As for resilience and business continuity, they are indeed offerring integrated paradigms that extend the risk one, and provide frameworks for more effectively coping with the uncertain nature and extent of emerging hazards, and their impacts on today’s complex, interconnected systems. Several concepts, definitions, models and techniques are emerging, all contributing insights into this difficult problem. Still advancements are needed, also with respect to how to manage resilience and business continuity from a design, normative and operational viewpoint, setting resilience goals, regulating resilience within a defence-in-depth safety approach and maintaining resilience margins during operation.

As for the safety and security of CPSs, the problem is of great relevance since these systems are applied everywhere, at every scale and every area, including aerospace, automotive, energy, chemical industry, materials, civil transportation, agriculture and healthcare. Examples are micro- and nano-scale cyber and physical materials, controlled components, cooperating medical devices and systems, next-generation power grids, future defense systems, next-generation automobiles and intelligent highways, flexible robotic manufacturing, next-generation air vehicles and airspace management, and so on. CPS integrate computing and communication capabilities with the monitoring and control of entities in the physical world, building a bridge between the cyber space and the physical space. A CPS is, then, a system of systems where there is a tight coupling between the computing components and the physical components, the underlying processes and the policies governing all this. The cyber part of the system demands security as one of its requirements; the physical part of the system requires safety. The system of systems combining the two parts requires both security and safety, and functional dependability. In CPSs, components are networked at every scale and each physical component has cyber capability. Computing is deeply embedded into every physical component. The behavior of a CPS is a fully integrated hybridization of computational (logical) and physical action. Moreover, the complete system has an excellent adaptability to the uncertain environment. While it is undoubtful that the new technologies will improve our lives, we must not understimate the risks and neglect the additional requirements that these bring. The high integration in the CPS has brought new risks as the physical components and systems can be malevolently accessed from the cyber space. With the integration of the cyber and physical spaces, the use of the general software, hardware, interfaces and protocols, the access to the internet etc., bring additional risks that must be considered. If the physical environment under control can be taken over by malicious entities, serious damage can occur. Besides the physical interferences, attacks, destructions to the physical components, what can be attacked is the information flow that runs them. An attacker could eavesdrop and tamper the sensor information, store information, control information, and even modify the logic of control algorithms. These can cause delays of the system, and even denial of service (DOS), which can pause the system operation. For instance, brief outages of critical infrastructures like the power grid may cause immeasurable losses and impacts. The suspension of a medical CPS may even be fatal. Therefore, we have to assess and demonstrate that our CPSs are dependable, safe, secure, besides being functional and efficient. To make CPSs resilient, it is necessary to integrate the knowledge on cyber security, human interactions and complex networks, to address all possible failure and threats in a comprehensive and holistic way. The aim is to design CPSs with the capabilities needed to operate safely and to survive the impacts of natural disasters, human errors, or intentional cyber attacks, with no loss of critical functions. For this, frameworks are needed that can combine simulation to recreate the physical components and processes, and emulation to recreate the cyber components and processes of networked industrial control systems such as SCADA servers and corporate networks. The framework should be flexible and adaptive to enable modifications, given that malevolent attacks and cyber threats keep changing to defeat the installed protections.

Other emergent topical aspects interwine with the discussions made in the paper. Some are worth at least a mention, because of their expected growing role in the development of the future of risk assessment and the bigger picture of future safety.

A first relevant topic is the growing awareness of the need for a concrete and practical method for accounting of safety mindfulness in operational situations (Weick et al. 2008). If the operators are aware of the potential threats that can occur during system operation, they can recognize and anticipate them. The challenge is in the management of the variety of risk information that can be utilized to the scope, including that coming from outside the local environment, e.g. across the industry. Some relevant information may take a long time to reach operators or concern new risks that may have been identified only by few involved parties, and formal processes of transmission are missing so that the needed information may not reach in time the operators who really need it: an incident could occur before existing processes have identified, analysed and processed such information, and disseminated it to the concerned operators. Fundamentally, safety mindfulness leads to being proactive, based on the best and most up-to-date information needed for carrying out the tasks related to the situation. It relies on the proper perception of the risk-relevant elements in the environment of interest, within a specified time and space domain, the correct comprehension of their meaning and the adequate projection of their status in the near future, to guide proper safety actions (Endsley, 1988). Mindfulness has become a quite popular concept for safety but has been difficult to implement, and so far there is no accepted measure of organizational mindfulness (Ray et. al., 2011). Concrete proposals on how to engineer mindfulness into organisations and processes are still needed.

Shifting along the risk profile from operational situations, and the need to recognize and anticipate risks, to emergency situations, the lessons learned from recent industrial accidents have confirmed the need to focus not only on the preventive measures that need to be designed for protection and on crisis management plans for mitigation, but also on the capacity to adapt in extreme situations that far exceed the scope of safety standards based on probabilistic risk assessment and on the comprehensive analysis of disaster scenarios. Crises in which conventional resources are lacking, but societal expectations are high, call for "engineering thinking in emergency situations" (Guarnieri and Travadel, 2014). This is a new concept that emphasizes adaptability and resilience within organizations—such as the ability to create temporary new organizational structures, to quickly switch from a normal state to an innovative mode and to integrate the social dimension into engineering activities. Future risk and resilience assessments will need to assess and demonstrate also the ability to create and implement effective engineering strategies on the fly, and the capability for resilience in the aftermath of accidents beyond design basis (those which defeat the designed protections and crisis management plans).

A last topic which seems worth mentioning, because emerging and expected to emerge even more in the developing “smart” technological World, is the social pressure and related behavioral influence that can be expected to affect the demand-response behaviour of socio-technical systems. More and more attention will need to be paid in risk (and resilience) assessments to the effects of the interwining of social media communication onto the operation of technical systems, with phenomena (e.g. of alert (positive effect) or fake news (negative effect) on hazards, dangers and opportunities, and others), which can deviate mass behavior of demand in operational and emergency situations, with effects on the operation and challenges to the capacity of response of the technical systems. Integration of these aspects in the risk and resilience assessment and management frameworks will become more and more necessary, and will require effective integration of different disciplines and competences.

In conclusion, the directions discussed in this paper are some relevant ones in which risk assessment is evolving and must continue to evolve for addressing the existing and future challenges, considering the new systems and innovations that are coming ahead. These directions all revolve around the knowledge at the basis of risk assessment and the modeling for organizing it in a structured, meaningful way. This involves the development of new methods and approaches, for which additional competences are required, e.g. in simulation and data analytics but also in social sciences. This is likely to change the framework of risk assessment and the related educational curricula for the preparation of the risk professionals of the future. In this view, the Society for Risk Analysis (SRA) Specialty Group on foundational issues in risk analysis and the SRA Committee for Specialty Groups have established a group of risk analysis experts with the mandate of producing a list of core subjects for the field (http://www.sra.org/frasg).

Acknowledgments: I am deeply grateful to Dr. Francesco Di Maio and Wei Wang of Politecnico di Milano, and Drs. Yiping Fang, Pietro Turati and Zhiguo Zeng of CentraleSupelec, Paris, and Nicola Pedroni of Politecnico di Torino, for their work that has greatly contributed to the substance of this paper. I am also grateful to the four anonymous reviewers, whose comments have allowed improving the paper significantly.

References

Finally, one could consider accidents and incidents as extreme states of behavior of these systems. An illustration of the use thereof see en Ale, Risk Analysis and Big Data, Safety and Reliability.2016 vol 36 no 3 153-165 DOI: 10.1080/09617353.2016.1252080; ISSN: 0961-7353 2469-4126

Abimbola, M., Khan, F., & Khakzad, N. (2014). Dynamic safety risk analysis of offshore drilling. Journal of Loss Prevention in the Process Industries, 30, 74-85.

Ahn, K. L., & Yang, J. E. (2003). The explicit treatment of model uncertainties in the presence of aleatory and epistemic parameter uncertainties in risk and reliability analysis. Nuclear Engineering and Technology, 35(1), 64-79.

Aldemir, T., Guarro, S., Mandelli, D., Kirschenbaum, J., Mangan, L.A., Bucci, P., Yau, M., Ekici, E., Miller, D.W., Sun, X. & Arndt, S.A. (2010). Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. Reliability Engineering & System Safety, 95(10), 1011-1039.

Aldemir, T. (2013). A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy, 52, 113-124.

Ale, B. (2016). Risk Analysis and Big Data. Reliability Engineering and System Safety, 36 (3), 153-165.

Alexander, R. and Kelly, T. (2013). Supporting systems of systems hazard analysis using multi-agent simulation. Safety Science, 51, 302-318.

Althoff, M., Stursberg, O., & Buss, M. (2007). safety Assessment of Autonomous Cars using Verification Techniques. In Proc. of the American Control Conference.

Alur, R., 2015. Principles of cyber-physical systems. MIT Press.

Amini, H., Cont, R., & Minca, A. (2013). Resilience to contagion in financial networks. Mathematical finance.

Apostolakis, G. E. (1990). The Concept of Probability in Safety Assessments of Technological Systems. Science, 250, 4986, 1359-1364.

Apostolakis, G. E. (2004). How useful is quantitative risk assessment?. Risk Analysis, 24, 3, 515-520.

Apostolakis, G. E. & Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis, 25(2), 361-376.

Attoh-Okine, N. O., Cooper, A. T., & Mensah, S. A. (2009). Formulation of resilience index of urban infrastructure using belief functions. IEEE Systems Journal, 3(2), 147-153.

Au, S. K., & Beck, J. L. (2003). Subset simulation and its application to seismic risk based on dynamic analysis. Journal of Engineering Mechanics, 129(8), 901-917.

Asnar, Y., & Giorgini, P. (2008, September). Analyzing business continuity through a multi-layers model. In International Conference on Business Process Management (pp. 212-227). Springer Berlin Heidelberg.

Aven, T. (2009). Identification of safety and security critical systems and activities. Reliability Engineering & System Safety, 94(2), 404-411.

Aven, T. (2010). Risk management. Springer Berlin Heidelberg.

Aven, T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Analysis, 31(4), 515-522.

Aven, T., & Zio, E. (2011). Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliability Engineering & System Safety, 96(1), 64-74.

Aven, T. (2012 a). The risk concept—historical and recent development trends. Reliability Engineering & System Safety, 99, 33-44.

Aven, T. (2012 b). Foundational issues in risk assessment and risk management. Risk Analysis, 32(10), 1647-1656.

Aven, T., Zio, E., Baraldi, P., & Flage, R. (2014). Uncertainty in Risk Assessment.

Aven, T., & Zio, E. (2014). Foundational issues in risk assessment and risk management. Risk Analysis, 34(7), 1164-1172.

Aven, T. (2016 a). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13.

Aven, T. (2016 b). Ignoring scenarios in risk assessments: Understanding the issue and improving current practice. Reliability Engineering & System Safety, 145, 215-220.

Aven, T., & Cox, L. A. (2016). National and Global Risk Studies: How Can the Field of Risk Analysis Contribute?. Risk Analysis, 36(2), 186-190.

Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., ... & Li, J. (2008, July). Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures. In Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE (pp. 1-8). IEEE.

Baraldi, P., Mangili, F., & Zio, E. (2012). A Kalman filter-based ensemble approach with application to turbine creep prognostics. IEEE Transactions on Reliability, 61(4), 966-977.

Baroud, H., Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2015). Inherent costs and interdependent impacts of infrastructure network resilience. Risk Analysis, 35(4), 642-662.

Bjerga, T., & Aven, T. (2016). Some perspectives on risk management: A security case study from the oil and gas industry. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 230(5), 512-520.

Bobbio, A., Bonanni, G., Ciancamerla, E., Clemente, R., Iacomini, A., Minichino, M., ... & Zendri, E. (2010). Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. Reliability Engineering & System Safety, 95(12), 1345-1357.

Bonafede, E. C., Cerchiello, P., & Giudici, P. (2007). Statistical models for business continuity management. Journal of Operational Risk, 2(4), 79-96.

Bradley, J.M. and Atkins, E.M., 2015. Optimization and control of cyber-physical vehicle systems. Sensors, 15(9), pp.23020-23049.

Bucklew, J. (2013). Introduction to rare event simulation. Springer Science & Business Media.

Boehmer, W., Brandt, C., & Groote, J. F. (2009, September). Evaluation of a business continuity plan using process algebra and modal logic. In Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference (pp. 147-152). IEEE.

Bonanno, G. A., Galea, S., Bucciarelli, A., & Vlahov, D. (2007). What predicts psychological resilience after disaster? The role of demographics, resources, and life stress. Journal of consulting and clinical psychology, 75(5), 671.

Botchkarev, O. & and Tripakis, S. (2000). Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations, in Hybrid Systems - Computation and Control, ser. LNCS 1790. Springer, 73–88.

Brandt, C., Hermann, F., & Engel, T. (2009, September). Modeling and reconfiguration of critical business processes for the purpose of a business continuity management respecting security, risk and compliance requirements at Credit Suisse using algebraic graph transformation. In Enterprise Distributed Object Computing Conference Workshops, 2009. EDOCW 2009. 13th (pp. 64-71). IEEE.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., ... & von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake spectra, 19(4), 733-752.

Bryson, K. M. N., Millar, H., Joseph, A., & Mobolurin, A. (2002). Using formal MS/OR modeling to support disaster recovery planning. European Journal of Operational Research, 141(3), 679-688.

Buzna, L., Peters, K., Ammoser, H., Kühnert, C., & Helbing, D. (2007). Efficient response to cascading disaster spreading. Physical Review E, 75(5), 056107.

Cadini, F., Santos, F., & Zio, E. (2014). An improved adaptive kriging-based importance technique for sampling multiple failure regions of low probability. Reliability Engineering & System Safety, *131*, 109-117. doi:10.1016/j.ress.2014.06.023.

Cadini, F., Gioletta, A. & Zio E. (2015). Improved metamodel-based importance sampling for the performance assessment of radioactive waste repositories.Reliability Engineering & System Safety 134: 188-197.

Çağnan, Z., Davidson, R. A., & Guikema, S. D. (2006). Post-earthquake restoration planning for Los Angeles electric power. Earthquake Spectra, 22(3), 589-608.

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: resilience of what to what?. Ecosystems, 4(8), 765-781.

Casari, M., & Wilkie, S. J. (2005). Sequencing lifeline repairs after an earthquake: an economic approach. Journal of Regulatory Economics, 27(1), 47-65.

Cimellaro, G. P., Reinhorn, A. M., Bruneau, M., & Rutenberg, A. (2006). Multidimensional fragility of structures: formulation and evaluation. Multidisciplinary Center for Earthquake Engineering Research, 123.

Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Framework for analytical quantification of disaster resilience. Engineering Structures, 32(11), 3639-3649.

Cérou, F., & Guyader, A. (2007). Adaptive multilevel splitting for rare event analysis. *Stochastic Analysis and Applications, 25*(2), 417-443.

Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. Information Systems Management, 21(3), 70-78.

Chang, J. I., & Lin, C. C. (2006). A study of storage tank accidents. Journal of loss prevention in the process industries, 19(1), 51-59.

Compare, M., Martini, F., Mattafirri, S., Carlevaro, F., & Zio, E. (2016). Semi-Markov model for the oxidation degradation mechanism in gas turbine nozzles. IEEE Transactions on Reliability, 65(2), 574-581.

Correa, G. J., & Yusta, J. M. (2013). Grid vulnerability analysis based on scale-free graphs versus power flow models. Electric Power Systems Research, 101, 71-79.

Cox Jr, L. A. (Ed.). (2015). Breakthroughs in Decision Science and Risk Analysis. John Wiley & Sons.

Cupac, V., Lizier, J. T., & Prokopenko, M. (2013). Comparing dynamics of cascading failures between network-centric and power flow models. International Journal of Electrical Power & Energy Systems, 49, 369-379.

Deng, Y., Li, Q., & Lu, Y. (2015). A research on subway physical vulnerability based on network theory and FMECA. Safety science, 80, 127-134.

Di Maio, F., Secchi, P., Vantini, S. & Zio, E. (2011). Fuzzy C-Means Clustering of Signal Functional Principal Components for Post-Processing Dynamic Scenarios of a Nuclear Power Plant Digital Instrumentation and Control System, IEEE Transactions on Reliability, Volume 60, no. 2, 415-425.

Di Muro, M. A., La Rocca, C. E., Stanley, H. E., Havlin, S., & Braunstein, L. A. (2015). Recovery of interdependent networks. arXiv preprint arXiv:1512.02555.

Dubois, D. (2006). Possibility theory and statistical reasoning. Computational statistics & data analysis, 51(1), 47-69.

Dubois, D. (2010). Representation, propagation, and decision issues in risk analysis under incomplete probabilistic information. Risk analysis, 30(3), 361-368.

Dueñas-Osorio, L., & Kwasinski, A. (2012). Quantification of lifeline system interdependencies after the 27 February 2010 Mw 8.8 offshore Maule, Chile, earthquake. Earthquake Spectra, 28(S1), S581-S603.

Dubi, A. (2010). Monte Carlo Applications in Systems Engineering, Wiley.

Eames, D.P. & Moffett, J. (1999), September. The integration of safety and security requirements. In International Conference on Computer Safety, Reliability, and Security (pp. 468-480). Springer Berlin Heidelberg.

Echard, B., Gayton, N., & Lemaire, M. (2011). AK-MCS: An active learning reliability method combining Kriging and Monte Carlo Simulation. *Structural Safety, 33*(2), 145-154.

Endsley, M. R. (1988). Situation awareness global assessment technique (SAGAT). In Proceedings of the National Aerospace and Electronics Conference. NAECON, 789-795.

Faertes, D. (2015). Reliability of supply chains and business continuity management. Procedia Computer Science, 55, 1400-1409.

Fan, M., Zeng, Z., Zio, E., & Kang, R. (2017). Modeling dependent competing failure processes with degradation-shock dependence. Reliability Engineering & System Safety.

Fang, Y. P., & Zio, E. (2013). Unsupervised spectral clustering for hierarchical modelling and criticality analysis of complex networks. Reliability Engineering & System Safety, 116, 64-74.

Fang, Y. P., Pedroni, N., & Zio, E. (2014). Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network. IEEE Systems Journal.

Fang, Y. & Sansavini, G. (2017). Optimizing power system investments and resilience against attacks. Reliability Engineering & System Safety, 159, 161-173.

Ferrario, E., & Zio, E. (2014). Goal Tree Success Tree–Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems. Engineering Structures, 59, 411-433.

Fiksel, J. (2003). Designing resilient, sustainable systems. Environmental science & technology, 37(23), 5330-5339.

Flage, R., Aven, T., Zio, E., & Baraldi, P. (2014). Concerns, challenges, and directions of development for the issue of representing uncertainty in risk assessment. Risk Analysis, 34(7), 1196-1207.

Flage, R., & Aven, T. (2015). Emerging risk–Conceptual definition and a relation to black swan type of events. Reliability Engineering & System Safety, 144, 61-67.

Guarro, S., Yau, M., Ozguner U., Aldemir, T., Kurt, A., Hejase, M. & Knudson M.D. (2107). Formal Framework and Models for Validation and Verification of Software-Intensive Aerospace Systems. Conference proceedings of AIAA SciTech Forum 2017, Grapevine, Texas.

Haimes, Y. Y. (2009). On the definition of resilience in systems. Risk Analysis, 29(4), 498-501.

Hameed, A., Khan, F., & Ahmed, S. (2016). A risk-based shutdown inspection and maintenance interval estimation considering human error. Process Safety and Environmental Protection, 100, 9-21.

Henry, D., & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering & System Safety, 99, 114-122.

Heo, G. (2016). Application of Dynamic PSA for Accident Sequence Precursor Analysis: Case Study for Steam Generator Tube Rupture. In the 13th International Conference on Probabilistic Safety Assessment and Management, Seoul, Korea.

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. Business history, 52(6), 978-1002.

Holling, C. S. (1973). Resilience and stability of ecological systems. Annual review of ecology and systematics, 4(1), 1-23.

Hollnagel, E. (2016). Resilience Engineering Perspectives, Volume 2: Preparation and Restoration. CRC Press.

Hu, X., Xu, M., Xu, S. & Zhao, P. (2017). Multiple cyber attacks against a target with observation errors and dependent outcomes: Characterization and optimization. Reliability Engineering & System Safety, 159, 119-133.

International Organization for Standardization (ISO) (2012), Societal security – business continuity management systems.

IRGC (2012). An introduction to the IRGC Risk Governance Framework, International Risk Governance Council, 2012 ISBN 978-2-9700772-2-0.

Inselberg, A. (2009). Parallel Coordinates: VISUAL Multidimensional Geometry and its Applications. Springer.

Jackson, S. (2007, June). 6.1. 3 System Resilience: Capabilities, Culture and Infrastructure. In INCOSE International Symposium (Vol. 17, No. 1, pp. 885-899).

Jiang, S., Zhang, W., He, J., & Wang, Z. (2016). Comparative study between crack closure model and Willenborg model for fatigue prediction under overload effects. Chinese Journal of Aeronautics, 29(6), 1618-1625.

Jin, J. G., Tang, L. C., Sun, L., & Lee, D. H. (2014). Enhancing metro network resilience via localized integration with bus services. Transportation Research Part E: Logistics and Transportation Review, 63, 17-30.

Jockenhövel-Barttfeld, M., Taurines, A. & Hessler, C. (2016). Quantification of Application Software Failures of Digital I&C in Probabilistic Safety Analyses. In 13th International Conference on Probabilistic Safety Assessment and Management, Seoul, Korea.

Johanson, G., & Holmberg, J. (1994). Safety evaluation by living probabilistic safety assessment. Procedures and applications for planning of operational activities and analysis of operating experience (No. SKI-R--94-2). Swedish Nuclear Power Inspectorate.

Kalantarnia, M., Khan, F., & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. Journal of Loss Prevention in the Process Industries, 22(5), 600-606.

Kalos, M.H. & Whitlock P. A. (2008). Monte Carlo Methods, 2nd Edition.

Kang, R., Zhang, Q., Zeng, Z., Zio, E., & Li, X. (2016). Measuring reliability under epistemic uncertainty: Review on non-probabilistic reliability metrics. Chinese Journal of Aeronautics, 29(3), 571-579.

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

Kelly, D. L., & Smith, C. L. (2009). Bayesian inference in probabilistic risk assessment—the current state of the art. Reliability Engineering & System Safety, 94(2), 628-643.

Kelly, D., & Smith, C. (2011). Bayesian inference for probabilistic risk assessment: A practitioner's guidebook. Springer Science & Business Media.

Khaitan, S.K. and McCalley, J.D., 2015. Design techniques and applications of cyberphysical systems: A survey. IEEE Systems Journal, 9(2), pp.350-365.

Khan, F., Rathnayaka, S., & Ahmed, S. (2015). Methods and models in process safety and risk management: past, present and future. Process Safety and Environmental Protection, 98, 116-147.

Khan, F., Hashemi, S. J., Paltrinieri, N., Amyotte, P., Cozzani, V., & Reniers, G. (2016). Dynamic risk management: a contemporary approach to process safety management. Current Opinion in Chemical Engineering, 14, 9-17.

Khakzad, N., Khan, F., & Amyotte, P. (2012). Dynamic risk analysis using bow-tie approach. Reliability Engineering & System Safety, 104, 36-44.

Khakzad, N., Khan, F., & Amyotte, P. (2013). Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety science, 57, 108-117.

Khakzad, N., Khan, F., & Amyotte, P. (2013b). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection, 91(1), 46-53.

Khakzad, N., Khan, F., & Paltrinieri, N. (2014). On the application of near accident data to risk analysis of major accidents. Reliability Engineering & System Safety, 126, 116-125.

Kim, K.D. and Kumar, P.R., 2012. Cyber–physical systems: A perspective at the centennial. Proceedings of the IEEE, 100(Special Centennial Issue), pp.1287-1308.

Kim, H., Lee, S. H., Park, J. S., Kim, H., Chang, Y. S., & Heo, G. (2015). Reliability data update using condition monitoring and prognostics in probabilistic safety assessment. Nuclear Engineering and Technology, 47(2), 204-211.

Kleijnen, J. P. C. (2009). Kriging metamodeling in simulation: A review. *European Journal of Operational Research*, *192*(3), 707-716.

Kozin, F., & Zhou, H. (1990). System study of urban response and reconstruction due to earthquake. Journal of Engineering Mechanics, 116(9), 1959-1972.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. and Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety, 139, pp.156-178.

Kröger, W., & Zio, E. (2011). Vulnerable systems. Springer Science & Business Media.

Labeau, P. E. (1996). Probabilistic dynamics: estimation of generalized unreliability through efficient Monte Carlo simulation. Annals of Nuclear Energy, 23(17), 1355-1369.

Lee, E.A., 2008, May. Cyber physical systems: Design challenges. In Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on (pp. 363-369). IEEE.

Lee II, E. E., Mitchell, J. E., & Wallace, W. A. (2007). Restoration of services in interdependent infrastructure systems: A network flows approach. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6), 1303-1317.

Lee, K. & Peng, H. (2005). Evaluation of automotive forward collision warn- ing and collision avoidance algorithms, Vehicle System Dynamics, vol. 43, no. 10, 735–751.

Léger, A. *et al.* (2009). Methodological developments for probabilistic risk analyses of socio-technical systems. *Proceedings of the Institution of Me- chanical Engineers, Part O: Journal of Risk and Reliability*, 223(4), 313-332.

Li, J., Mosleh, A., & Kang, R. (2010). *From blind to guided simulation: Biased monte carlo based on entropy and zero variance for dynamic PSA applications.* Paper presented at the 10th International Conference on Probabilistic Safety Assessment and Management 2010, PSAM 2010.

Li, X., Chen, G., & Zhu, H. (2016). Quantitative risk analysis on leakage failure of submarine oil and gas pipelines using Bayesian network. Process Safety and Environmental Protection, 103, 163-173.

Liang, G., Zhao, J., Luo, F., Weller, S. & Dong, Z.Y. (2017). A review of false data injection attacks against modern power systems. IEEE Transactions on Smart Grid.

Liu, G., & Ji, C. (2007). Resilience of all-optical network architectures under in-band crosstalk attacks: a probabilistic graphical model approach. IEEE Journal on Selected Areas in Communications, 25(3).

Lin, Y. H., Li, Y. F., & Zio, E. (2015). Integrating random shocks into multi-state physics models of degradation processes for component reliability assessment. IEEE Transactions on Reliability, 64(1), 154-166.

Liu, S., Maljovec, D., Wang, B., Bremer, P. T., & Pascucci, V. (2017). Visualizing high-dimensional data: Advances in the past decade. IEEE Transactions on Visualization and Computer Graphics, 23(3), 1249-1268.

Ma Z., Smith C., Prescott S. (2017a) A Simulation-Based Dynamic Approach for External Flooding Analysis in Nuclear Power Plants. In: Jiang H. (eds) Proceedings of The 20th Pacific Basin Nuclear Conference. PBNC 2016. Springer, Singapore.

Ma Z., Smith C. & Prescott S. (2017b). A Case Study of Simulation-Based Dynamic Analysis Approach for Modeling Plant Response to Flooding Events. In the 2017 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA2017), Pittsburgh, USA.

Machado, R.C., Boccardo, D.R., De Sá, V.G.P. & Szwarcfiter, J.L. (2016). Software control and intellectual property protection in cyber-physical systems. EURASIP Journal on Information Security, 2016(1), pp.1-14.

Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. IEEE Systems Journal, 3(2), 181-191.

Mandelli, D., Yilmaz, A., Aldemir, T., Metzroth, K., Denning, R. (2013a). Scenario clustering and dynamic probabilistic risk assessment, Reliability Engineering & System Safety, 115, 146-160.

Mandelli, D., Smith, C., Rabiti, C., Alfonsi, A., Youngblood, R., Pascucci, V., ... & Yilmaz, A. (2013b). Dynamic PRA: an overview of new algorithms to generate, analyze and visualize data. Proceeding of American Nuclear Society.

Mandelli, D., Smith, C., Riley, T., Nielsen, J., Alfonsi, A., Cogliati, J., Rabiti, C. & Schroeder J. (2016) BWR Station Blackout: A RISMC Analysis Using RAVEN and RELAP5-3D, Nuclear Technology, 193:1, 161-174

Maljovec, D., Liu, S., Wang, S., Mandelli, D., Bremer, P.-T., Pascucci, V., Smith, C. (2016). Analyzing simulation-based PRA data through traditional and topological clustering: A BWR station blackout case study, Reliability Engineering & System Safety, 145, 262–276

Marseguerra, M., & Zio, E. (1996). Monte Carlo approach to PSA for dynamic process systems. Reliability Engineering & System Safety, 52(3), 227-241.

Matisziw, T. C., Murray, A. T., & Grubesic, T. H. (2010). Strategic network restoration. Networks and Spatial Economics, 10(3), 345-361.

McNelles, P., Zeng, Z.C., Renganathan, G., Lamarre, G., Akl, Y. & Lu, L. (2016). A comparison of Fault Trees and the Dynamic Flowgraph Methodology for the analysis of FPGA-based safety systems Part 1: Reactor trip logic loop reliability analysis. Reliability Engineering & System Safety, 153, 135-150.

Meel, A., & Seider, W. D. (2006). Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science, 61(21), 7036-7056.

Meel, A., & Seider, W. D. (2008). Real-time risk analysis of safety systems. Computers & Chemical Engineering, 32(4), 827-840.

Meng, Y., Lu, C., Yan, Y., Shi, L., & Liu, J. (2015). Method to analyze the regional life loss risk by airborne chemicals released after devastating earthquakes: A simulation approach. Process Safety and Environmental Protection, 94, 366-379.

Mohammadpourfard, M., Sami, A. & Seifi, A.R. (2017). A statistical unsupervised method against false data injection attacks: A visualization-based approach. Expert Systems with Applications, 84, 242-261.

Moteff J.D. (2012) “Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress,” Congressional Res. Service.

Montero-Mayorga, J., Queral, C., & Gonzalez-Cadelo, J. (2014). Effects of delayed RCP trip during SBLOCA in PWR. Annals of Nuclear Energy, 63, 107-125.

Munoz Zuniga, M., Garnier, J., Remy, E., & De Rocquigny, E. (2011). Adaptive directional stratification for controlled estimation of the probability of a rare event. Reliability Engineering and System Safety, *96*(12), 1691-1712.

National Academy Press, Committee on the Institutional Means for Assessment of Risks to Public Health, National Research Council (1983). Risk Assessment in the Federal Government: Managing the Process.

Najjar, W., & Gaudiot, J. L. (1990). Network resilience: A measure of network fault tolerance. IEEE Transactions on Computers, 39(2), 174-181.

NASA (2013). rContext-Based Software Risk Model (CSRM) Application Guide, NASA/CR-2013-218111, NASA Headquarters, Washington, D.C.

Necci, A., Antonioni, G., Cozzani, V., Krausmann, E., Borghetti, A., & Nucci, C. A. (2013). A model for process equipment damage probability assessment due to lightning. Reliability Engineering & System Safety, 115, 91-99.

Necci, A., Argenti, F., Landucci, G., & Cozzani, V. (2014). Accident scenarios triggered by lightning strike on atmospheric storage tanks. Reliability Engineering & System Safety, 127, 30-46.

Newman, L., & Dale, A. (2005). Network structure, diversity, and proactive resilience building: a response to Tompkins and Adger. Ecology and society, 10(1).

NODA, S., & KANO, H. (1993). Hypocenter estimation system for earthquake countermeasures. Journal of natural disaster science, 15(1), 53-90.

NRC (1975) Reactor Safety Study, an Assessment of Accident Risks. Wash 1400. Report NUREG-75/014. Washington, D.C. U.S. Nuclear Regulatory Commission.

Ntalampiras, S. (2015). Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling. IEEE Transactions on Industrial Informatics, 11(1), 104-111.

Ntalampiras, S. (2016). Automatic identification of integrity attacks in cyber-physical systems. Expert Systems with Applications, 58, 164-173.

NUREG (1983) . PRA procedures guide, vols. 1&2, NUREG/CR-2300, January 1983.

NUREG-1150, 1990. Severe accident risk: an assessment for five US nuclear power plants, US Nuclear Regulatory Commission.

NUREG-CR-6850, 2005. EPRI/NRC-RES Fire PRA methodology for nuclear power facilities, Volume 2: detailed methodology. US Nuclear Regulatory Commission.

Obama B. (2013) “Presidential Policy Directive 21: Critical Infrastructure Security and Resilience,” Washington, DC, USA.

Omer, M., Nilchiani, R., & Mostashari, A. (2009). Measuring the resilience of the trans-oceanic telecommunication cable system. IEEE Systems Journal, 3(3), 295-303.

Ouyang, M., Hong, L., Mao, Z. J., Yu, M. H., & Qi, F. (2009). A methodological approach to analyze vulnerability of interdependent infrastructures. Simulation Modelling Practice and Theory, 17(5), 817-828.

Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. Structural safety, 36, 23-31.

Östergaard, C., Dogliani, M., Guedes Soares, C., Parmentier, G. and Pedersen, P.T. (1996). Measures of model uncertainty in the assessment of primary stresses in ship structures. Marine Structures, 9, 427-447.

Papazoglou, I.A., Ale, B.J.M. (2007). A logical model for quantification of occupational risk. Reliability Engineering & System Safety, 92 (6), 785-803.

Papazoglou, I.A., Aneziris, O., Bellamy, L.J., Damen, M., Ale, B.J.M., Manuel, H.J. Oh, J.I.H. (2015). Uncertainty assessment in the quantification of risks rates of occupational accidents. Risk Analysis, Vol. 35 (8).

Parry, G. and Winter P.W. (1981) Characterization and evaluation of uncertainty in probabilistic risk analysis. Nuclear Safety 22(1), 28-42.

Parise, G., Hesla, E., Parise, L., & Pennacchia, R. (2016). Switching procedures and business continuity management: The flock logic of multiple source systems. IEEE Transactions on Industry Applications, 52(1), 60-66.

Pariyani, A., Seider, W. D., Oktem, U. G., & Soroush, M. (2012). Dynamic risk analysis using alarm databases to improve process safety and product quality: Part II—Bayesian analysis. AIChE Journal, 58(3), 826-841.

Paltrinieri, N., Khan, F., Amyotte, P., & Cozzani, V. (2014). Dynamic approach to risk management: application to the Hoeganaes metal dust accidents. Process Safety and Environmental Protection, 92(6), 669-679.

Pedroni, N., Zio, E., Pasanisi, A., & Couplet, M. (2017). A Critical Discussion and Practical Recommendations on Some Issues Relevant to the Nonprobabilistic Treatment of Uncertainty in Engineering Risk Assessment. Risk Analysis.

Piètre-Cambacédès, L. and Bouissou, M., 2013. Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety, 110, pp.110-126.

Praks, P., Kopustinskas, V., & Masera, M. (2015). Probabilistic modelling of security of supply in gas networks and evaluation of new infrastructure. Reliability Engineering & System Safety, 144, 254-264.

Pursiainen, C. (2009). The challenges for European critical infrastructure protection. European Integration, 31(6), 721-739.

Rabbani, M., Soufi, H. R., & Torabi, S. A. (2016). Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery. Safety Science, 85, 9-22.

Rae, A., McDermid, J. and Alexander, R. (2012). In Proceedings of PSAM 11 and ESREL 2012, 2292-2301.

Rahman, M.S., Mahmud, M.A., Oo, A.M. & Pota, H.R. (2016). Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems. IEEE Transactions on Industrial Informatics, 1-10.

Ray, J. L., Baker, L. T., & Plowman, D. A. (2011). Organizational Mindfulness in Business Schools. Academy of Management Learning & Education, 10(2), 188-203.

Reed, D. A., Kapur, K. C., & Christie, R. D. (2009). Methodology for assessing the resilience of networked infrastructure. IEEE Systems Journal, 3(2), 174-180.

Roy, A., Srivastava, P., & Sinha, S. (2015). Dynamic failure assessment of an ammonia storage unit: A case study. Process Safety and Environmental Protection, 94, 385-401.

Reid, S.G (1992) Acceptable risk. In: D.I. Blockley, Editor, Engineering Safety, McGraw-Hill, New York, pp. 138–166.

Reniers, G. L., & Audenaert, A. (2014). Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures wrt domino effects. Process Safety and Environmental Protection, 92(6), 583-589.

Renn, O. (1998) Three decades of risk research: accomplishments and new challenges, Journal of Risk Research 1 (1), 49–71 (1998).

Rechard, R.P.. (1999) Historical relationship between performance assessment for radioactive waste disposal and other types of risk assessment. Risk Analysis, 19(5):763-807.

Rechard, R.P. (2000) Historical background on performance assessment for the waste isolation pilot plant, Reliability Engineering and System Safety, 69 (3), 5-46.

Robert, C., & Casella, G. (2004). Monte Carlo Statistical Methods Springer-Verlag. New York.

Rosenkrantz, D. J., Goel, S., Ravi, S. S., & Gangolly, J. (2009). Resilience metrics for service-oriented networks: A service allocation approach. IEEE Transactions on Services Computing, 2(3), 183-196.

Rubino, G., & Tuffin, B. (Eds.). (2009). Rare event simulation using Monte Carlo methods. John Wiley & Sons.

Rubinstein, R. Y. & Kroese, D. P. (2016). Simulation and the Monte Carlo Method, Wiley.

Rumsfeld (2002) DoD News Briefing - Secretary Rumsfeld and Gen. Myers. Available online from: http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

Rose, A. Z. (2009). Economic resilience to disasters.

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261-273.

Sansavini, G., Piccinelli, R., Golea, L. R., & Zio, E. (2014). A stochastic framework for uncertainty analysis in electric power transmission systems with wind generation. Renewable Energy, 64, 71-81.

Santner, T. J., Williams, B. J., & Notz, W. I. (2003). The Design and Analysis of Computer Experiments Springer-Verlag. New York.

Shin, J., Son, H. & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. Reliability Engineering & System Safety, 134, 208-217.

Shinozuka, M., Chang, S. E., Cheng, T. C., Feng, M., O'Rourke, T. D., Saadeghvaziri, M. A., ... & Shi, P. (2004). Resilience of integrated power and water systems. Seismic Evaluation and Retrofit of Lifeline Systems, Articles from MCEER's Research Progress and Accomplishments Volumes, 65-86.

Siu, N. (1994). Risk assessment for dynamic systems: an overview. Reliability Engineering & System Safety, 43(1), 43-73.

Simpson, T. W., Poplinski, J. D., Koch, P. N., & Allen, J. K. (2001). Metamodels for computer-based engineering design: survey and recommendations. Engineering with computers, 17(2), 129-150.

Snedaker, S. (2013). Business continuity and disaster recovery planning for IT professionals. Newnes.

Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise resilience: managing risk in the networked economy. Strategy and Business, 30, 70-79.

Han, X. F., Li, J. S., Bi, Y. M., & Sun, M. D. (2005). Design and Realization of Landmark Matching Algorithm for UAV Based on Cluster System. MINIMICRO SYSTEMS-SHENYANG-, 26(5), 841.

Tan, Y., & Takakuwa, S. (2011). Use of simulation in a factory for business continuity planning. International Journal of Simulation Modelling, 10(1), 17-26.

Tan, R., Nguyen, H.H., Foo, E.Y., Yau, D.K., Kalbarczyk, Z., Iyer, R.K. & Gooi, H.B. (2017). Modeling and Mitigating Impact of False Data Injection Attacks on Automatic Generation Control. IEEE Transactions on Information Forensics and Security, 12(7), 1609-1624.

Taleb, N. (2007). The black swan: the impact of the highly improbable. Random House, 401.

Tierney, K., & Bruneau, M. (2007). Conceptualizing and measuring resilience: A key to disaster loss reduction. TR news, (250).

Trabelsi, Z. & Rahmani, H. (2005). An Anti-Sniffer Based on ARP Cache Poisoning Attack. Information Systems Security, 13(6), 23-36.

Turati, P., Pedroni, N., & Zio, E. (2016 a). Advanced RESTART method for the estimation of the probability of failure of highly reliable hybrid dynamic systems. Reliability Engineering & System Safety, 154, 117-126.

Turati, P., Pedroni, P. & Zio E. (2016 b). Dimensionality reduction of the resilience model of a critical infrastructure network by means of elementary effects sensitivity analysis. European Safety and RELiability Conference (ESREL) 2016, Sep 2016, Glasgow, United Kingdom. pp.2797-2804, 2017, Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016.

Turati, P., Pedroni, N., & Zio, E. (2017). An adaptive simulation framework for the exploration of extreme and unexpected events in dynamic engineered systems. Risk analysis, 37(1), 147-159.

Todini, E. (2000). Looped water distribution networks design using a resilience index based heuristic approach. Urban water, 2(2), 115-122.

Tomlin, C., Mitchell, I., Bayen, A. & Oishi, M. (2003) Computational techniques for the verification and control of hybrid systems, in Proceedings of the IEEE, vol. 91, 986–1001.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. Safety science, 89, 201-218.

Trucco, P., & Leva, M. C. (2012). BN Applications in Operational Risk Analysis: Scope, Limitations and Methodological Requirements. INTECH Open Access Publisher.

Valdebenito, M. A., Pradlwarter, H. J., & Schuëller, G. I. (2010). The role of the design point for calculating failure probabilities in view of dimensionality and structural nonlinearities. Structural Safety, 32(2), 101-111.

van der Schaft, A. & Schumacher, H. (2000), An Introduction to Hybrid Dynamical Systems. Springer.

Villa, V., Paltrinieri, N., Khan, F., & Cozzani, V. (2016). Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. Safety science, 89, 77-93.

Villén-Altamirano, M., & Villén-Altamirano, J. (1991). RESTART: A method for accelerating rare event simulations. Analysis, 3, 3.

Wang, H., Khan, F., Ahmed, S., & Imtiaz, S. (2016). Dynamic quantitative operational risk assessment of chemical processes. Chemical Engineering Science, 142, 62-78.

Wang, W., Di Maio, F. & Zio, E. (2016b). Component-and system-level degradation modeling of digital Instrumentation and Control systems based on a Multi-State Physics Modeling Approach. Annals of Nuclear Energy, 95, pp.135-147.

Wang, W., Cammi, A., Di Maio F., Lorenzi, S. & Zio, E. (2017). A Probabilistic Modelling and Simulation Framework for Identifying Components Vulnerable to Cyber Threats in Nuclear Power Plants. Submitted to Reliability Engineering & System Safety.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. Crisis management, 3, 81-123.

Wreathall, J. (2006). Developing models for measuring resilience. John Wreathall & Co., Inc., Dublin, Ohio.

Wu, D., & Chen, Z. (2016). Quantitative risk assessment of fire accidents of large-scale oil tanks triggered by lightning. Engineering Failure Analysis, 63, 172-181.

Xiang, Y., Wang, L. & Liu, N. (2017). Coordinated attacks on electric power systems in a cyber-physical environment. Electric Power Systems Research, 149, 156-168.

Xu, N., Guikema, S. D., Davidson, R. A., Nozick, L. K., Çağnan, Z., & Vaziri, K. (2007). Optimizing scheduling of post-earthquake electric power restoration tasks. Earthquake engineering & structural dynamics, 36(2), 265-284.

Yadav, V., Agarwal, V., Gribok, A.V. & Smith, C.L. (2017). Dynamic PRA with Component Aging and Degradation Modeled Utilizing Plant Risk Monitoring Data. In the 2017 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA2017), Pittsburgh, USA.

Yamaguchi, A., Jang, S., Hida, K., Yamanaka, Y., & Narumiya, Y. (2017). Risk Assessment Strategy for Decommissioning of Fukushima Daiichi Nuclear Power Station. Nuclear Engineering and Technology, 49(2), 442-449.

Yang, J. E. (2014). Fukushima Dai-Ichi accident: lessons learned and future actions from the risk perspectives. Nuclear Engineering and Technology, 46(1), 27-38.

Yang, M., Khan, F. I., & Lye, L. (2013). Precursor-based hierarchical Bayesian approach for rare event frequency estimation: a case of oil spill accidents. Process safety and environmental protection, 91(5), 333-342.

Yang, M., Khan, F., Lye, L., & Amyotte, P. (2015). Risk assessment of rare events. Process Safety and Environmental Protection, 98, 102-108.

Yu, H., Khan, F., Garaniya, V., & Ahmad, A. (2014). Self-organizing map based fault diagnosis technique for non-Gaussian processes. Industrial & Engineering Chemistry Research, 53(21), 8831-8843.

Yuan, Y., Zhu, Q., Sun, F., Wang, Q. & Başar, T. (2013). Resilient control of cyber-physical systems against denial-of-service attacks. In Resilient Control Systems (ISRCS), 2013 6th International Symposium on (pp. 54-59). IEEE.

Yuan, W., Zhao, L. & Zeng, B. (2014). Optimal power grid protection through a defender–attacker–defender model. Reliability Engineering & System Safety, 121, 83-89.

Zadakbar, O., Imtiaz, S., & Khan, F. (2012). Dynamic risk assessment and fault detection using principal component analysis. Industrial & Engineering Chemistry Research, 52(2), 809-816.

Zadakbar, O., Imtiaz, S., & Khan, F. (2013). Dynamic risk assessment and fault detection using a multivariate technique. Process Safety Progress, 32(4), 365-375.

Zadakbar, O., Khan, F., & Imtiaz, S. (2015). Dynamic Risk Assessment of a Nonlinear Non-Gaussian System Using a Particle Filter and Detailed Consequence Analysis. The Canadian Journal of Chemical Engineering, 93(7), 1201-1211.

Zalewski, J., Buckley, I.A., Czejdo, B., Drager, S., Kornecki, A.J. and Subramanian, N., 2016. A Framework for Measuring Security as a System Property in Cyberphysical Systems. Information, 7(2), p.33.

Zargar, S.T., Joshi, J. & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), 2046-2069.

Zarei, E., Azadeh, A., Khakzad, N., Aliabadi, M. M., & Mohammadfam, I. (2017). Dynamic safety assessment of natural gas stations using Bayesian network. Journal of hazardous materials, 321, 830-840.

Zaytoon, J. & Lafortune, S. (2013). Overview of fault diagnosis methods for discrete event systems. Annual Reviews in Control, 37(2), 308-320.

Zeng, Z., Kang, R., & Chen, Y. (2014). A physics-of-failure-based approach for failure behavior modeling: With a focus on failure collaborations. In Proceedings of Annual European Safety and Reliability Conference (ESREL2014). Piscataway, NJ: IEEE Press (pp. 1-9).

Zeng, Z., Kang, R., & Chen, Y. (2016). Using PoF models to predict system reliability considering failure collaboration. Chinese Journal of Aeronautics, 29(5), 1294-1301.

Zeng, Z., & Zio, E. (2017). An integrated modeling framework for quantitative business continuity assessment. Process Safety and Environmental Protection, 106, 76-88.

Zeng, Z., & Zio, E. (2017b). Dynamic risk assessment based on statistical failure data and condition-monitoring degradation data. IEEE Transactions on Reliability, Under review.

Zhang, X., Miller-Hooks, E., & Denny, K. (2015). Assessing the role of network topology in transportation network resilience. Journal of Transport Geography, 46, 35-45.

Zheng, X., Yamaguchi, A., & Takata, T. (2014). Quantitative common cause failure modeling for auxiliary feedwater system involving the seismic-induced degradation of flood barriers. Journal of Nuclear Science and Technology, 51(3), 332-342.

Zhou, J., Reniers, G., & Khakzad, N. (2016). Application of event sequence diagram to evaluate emergency response actions during fire-induced domino effects. Reliability Engineering & System Safety, 150, 202-209.

Zio, E. (2007). An introduction to the basics of reliability and risk analysis (Vol. 13). World scientific.

Zio, E. (2009). Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety, 94(2), 125-141.

Zio, E. & Di Maio, F. (2009). Processing dynamic scenarios from a reliability analysis of a nuclear power plant digital instrumentation and control system. Annals of Nuclear Energy, 36(9), 1386-1399.

Zio, E., & Aven, T. (2011). Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?. Energy Policy, 39(10), 6308-6320.

Zio, E., & Sansavini, G. (2011). Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Transactions on Reliability, 60(1), 94-101.

Zio, E. (2013). The Monte Carlo simulation method for system reliability and risk analysis (p. 198p). London: Springer.

Zio, E. (2014). Integrated deterministic and probabilistic safety assessment: concepts, challenges, research directions. Nuclear Engineering and Design, 280, 413-419.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137-150.

Zio, E. (2016b). Reliability Analysis of Systems of Systems. IEEE Reliab. Mag, 1-6.

Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. Decision Support Systems, 50(2), 394-403.

Zsidisin, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. International journal of production research, 43(16), 3401-3420.