Enrico Zio

COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS

Series on Quality, Reliability and Engineering Statistics **Vol. 14**

COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS

Enrico Zio
Polytechnic of Milan, Italy

World Scientific

COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS

SERIES ON QUALITY, RELIABILITY AND ENGINEERING STATISTICS

Series Editors: M. Xie (National University of Singapore)
T. Bendell (Nottingham Polytechnic)
A. P. Basu (University of Missouri)

Published

To Sleeping Beauty, Snowhite and Saetta Mc Queen
To my wife Giorgia, author of my life book

Milano, 20 July 2008

Reliability and safety are fundamental attributes of any modern technological system. In practice, diverse types of protection barriers are placed as safeguards from the hazard posed by the system operation, within a *multiple-barrier* concept. These barriers are intended to protect the system from failures of any of its components, hardware, software, human and organizational.

Correspondingly, the reliability and risk analyses of a given system aim at the quantification of the probability of failure of the system itself and of its protective barriers.

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

One classical way to defend a system beyond the uncertainty of its failure scenarios has been to:

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

Within this *structuralist, defense-in-depth* approach, safety margins against these scenarios are enforced through conservative regulations of system design and operation, under the creed that the identified worst-case, credible accidents would envelope all credible accidents for what regards the challenges and stresses posed onto the system and its protections. The underlying principle has been that if a system is designed to withstand all the worst-case credible accidents, then it is 'by definition' protected against any credible accident [1].

This approach has been the one classically undertaken, and in many technological instances it still is, to protect a system from the uncertainty of the unknown failure behaviours of its components, systems and structures, without directly quantifying it, so as to provide reasonable

assurance that the system can be operated without undue risk. However, the practice of referring to "worst" cases implies subjectivity and arbitrariness in the definition of the accidental events, which may lead to the consideration of scenarios characterized by really catastrophic consequences, although highly unlikely. This may lead to the imposition of unnecessarily stringent regulatory burdens and thus excessive conservatism in the design and operation of the system and its protective barriers, with a penalization of the industry. This is particularly so for those industries, such as the nuclear, aerospace and process ones, in which accidents may lead to potentially large consequences.

For this reason, a more rational and quantitative approach has been pushed forward for the design, regulation and management of the safety of hazardous systems. This approach, initially motivated by the growing use of nuclear energy and by the growing investments in aerospace missions in the 1960s, stands on the principle of looking quantitatively also at the reliability of the accident-preventing and consequence-limiting protection systems which intervene in all potential accident scenarios, in principle with no longer any differentiation between credible and incredible, large and small accidents [2]. Initially, a number of studies were performed for investigating the merits of a quantitative approach based on probability for the treatment of the uncertainty associated with the occurrence and evolution of accident scenarios [3]. The findings of these studies motivated the first complete and full-scale probabilistic risk assessment of a nuclear power installation [4]. This extensive work showed that indeed the dominant contributors to risk need not be necessarily the design-basis accidents, a 'revolutionary' discovery undermining the fundamental creed underpinning the structuralist, defense-in-depth approach to safety [1].

Following these lines of thought, the probabilistic approach to risk analysis (PRA) has arisen as an effective way for analysing system safety, not limited only to the consideration of worst-case accident scenarios but extended to looking at all feasible scenarios and its related consequences, with the probability of occurrence of such scenarios becoming an additional key aspect to be quantified in order to rationally and quantitatively handle uncertainty [4-11]. From the view point of safety regulations, this has led to the introduction of new criteria which account for both the consequences of the scenarios and their probabilities

of occurrence under a now *rationalist,* defense-in-depth approach. Within this approach to safety analysis and regulation, reliability engineering takes on a most relevant role in the assessment of the probability of occurrence of the accident scenarios.

In this book, a number of methods for computing the reliability and risk characteristics of complex technological systems are illustrated. The presentation of the theory behind the methods is of pedagogical nature, but supported with practical examples for a clearer understanding of how these methods can be applied in the field.

Chapter 1 introduces the basics of the Markov approach to system modeling for reliability and availability analysis. In this approach, the stochastic process of evolution of the system in time is described through the definition of the system states, the possible transitions among these states and their probabilities of occurrence. The various system states are defined in terms of the states of the components comprising the system. The components are not restricted to having only two possible states but rather may have a number of different states such as functioning, in standby, degraded, partially failed, completely failed, under maintenance, etc.; the various failure modes of a component may also be defined as states. The transitions between the states occur randomly in time, because caused by various mechanisms and activities such as failures, repairs, replacements and switching operations, which are random in nature. Under specified conditions, the stochastic process of the system evolution may be described as a so called Markov process which is mathematically described by a system of probability equations which can be solved analytically or numerically.

Chapter 2 gives a short introduction to the theory of Monte Carlo simulation for reliability and availability analysis. The presentation is kept at an intuitive and practical level. The Monte Carlo simulation method is shown to offer a powerful tool which can be of great value in the analysis of complex systems, due to its inherent capability of achieving a closer adherence to reality in the representation of the system stochastic behaviour. In general terms, it may be defined as a methodology for obtaining estimates of the solution of mathematical problems by means of random numbers. By random numbers we mean numbers obtained through a roulette-like machine of the kind utilized in the gambling casinos at the Montecarlo Principate: hence the name of the

method. The random sampling of numbers was utilized in the past, well before the development of the present computers, by skillful scientists. The first example of use of what we now call Monte Carlo method seems to go back to the French naturalist Buffon (1707-88) who considered a set of parallel straight lines a distance D apart onto a plane and computed the probability P that a segment of length $L < D$ randomly positioned on the plane would intersect one of these lines. The theoretical expression he obtained was

$$P = \frac{L/D}{\pi/2}$$

Possibly not completely convinced about the correctness of his result, Buffon had the idea of checking the above expression by actually drawing parallel lines and repeatedly throwing a needle on the floor of his house to experimentally estimate the probability P as the ratio of the number of intersections to the total number of throws, thus acquiring the honour of being the inventor of the Monte Carlo method. It is interesting to mention that, later on, Laplace noticed that the Buffon's experiment represented a device for computing π just by throwing a needle on a floor with parallel lines. Successively other scientists used similar methods to solve integrals and probability problems. Eventually, the revival of the method seems to be ascribed to Fermi, von Neumann and Ulam in the course of the Manhattan Project during World War II. Back then, the Monte Carlo method provided the only option for solving the six-dimensional integral equations employed in designing shielding for nuclear devices. It was probably the first case in human history in which solutions based on trial and error were clearly too risky. Currently, Monte Carlo simulation seems to be the only method that can yield solutions to complex multi-dimensional problems. For about three decades it was used almost exclusively, and extensively, in nuclear technology. Presumably, the main reason for its use being limited to only nuclear applications was the lack of suitable computing power: indeed, the method is computer memory- and time-intensive. With the increasing availability of fast computers the application of the method becomes more and more feasible in the practice of various fields, including reliability and risk analysis.

Chapter 3 combines the modeling power of the Markov approach with the computing power of Monte Carlo simulation. This gives rise to the so called Markov Chain Monte Carlo techniques which offer an effective way for sampling from complicated probability distributions in high-dimensional spaces. This is useful in such tasks as image reconstruction, parameter identification, computing the equilibrium distribution and associated energy levels of statistical mechanics systems, inverse problem solving and more generally Bayesian posterior inference. Examples of application are provided with respect to the characterization of the failure and degradation behaviours of components and structures.

Chapter 4 illustrates the use of Genetic Algorithms within the area of RAMS (Reliability, Availability, Maintainability and Safety) optimization. The theory behind the operation of genetic algorithms is presented. The steps of the algorithm are sketched to some details for both the traditional breeding procedure as well as for more sophisticated breeding procedures. The necessity of affine transforming the fitness function, object of the optimization, is discussed in detail, together with the transformation itself. Finally, two examples of application are illustrated with regards to problems of reliability allocation and periodic inspection and maintenance. RAMS optimization is classically based on quantifying the effects that design and operation choices and testing and maintenance activities have on a number of system attributes like:

- $R(\underline{x})$ = System Reliability;

- $A(\underline{x})$ = System Availability ($U(\underline{x})$= system unavailability $=1 - A(\underline{x})$);

- $M(\underline{x})$ = System Maintainability, i.e. the unavailability contribution due to test and maintenance;

- $S(\underline{x})$ = System Safety, normally quantified in terms of the system risk measure $Risk(\underline{x})$ (e.g. as assessed from a Probabilistic Risk Analysis);

where $\underline{x}$ represents the vector of the design, operation and maintenance decision variables. A quantitative model is used to asses how the design, operation and maintenance choices affect the system RAMS attributes and the

involved costs (C($\underline{x}$) = Cost required to implement the vector choice $\underline{x}$). Thus, the design, operation and maintenance optimization problem must be framed as a multiple criteria decision making problem where RAMS&C attributes act as the conflicting decision criteria with the respect to which optimization is sought and the relevant design and maintenance parameters (e.g. redundancy configuration, component failure rates, maintenance periodicities, testing frequencies) act as the decision variables $\underline{x}$. Then, the multiple criteria decision-making analysis aims at finding the appropriate choices of reliability design, testing and maintenance procedures that optimally balance the conflicting RAMS and Costs (RAMS&C) attributes. In this general view, the vector of the decision variables $\underline{x}$ encodes the parameters related to the inherent equipment reliability (e.g. per demand failure probability, failure rate, etc.) and to the system logic configuration (e.g. number of redundant trains, etc.), which define the system reliability allocation, and those relevant to testing and maintenance activities (test intervals, maintenance periodicities, renewal periods, maintenance effectiveness, mean repair times, allowed downtimes, etc...) which govern the system availability and maintainability characteristics.

Chapter 5 investigates the issues related to dependent failures and illustrates the approaches used to model their effects on system reliability. This is a quite crucial issue in reliability and risk analysis since in spite of the fact that all modern technological systems are highly redundant, they still fail because of dependent failures which can defeat the redundant system protective barriers and thus contribute significantly to risk; quantification of such contribution is thus necessary to avoid gross underestimation of risk.

Chapter 6 is devoted to the presentation of the concept of importance measure in reliability and risk analysis. From a broad perspective, importance measures aim at quantifying the contribution of components to the system performance, e.g. its reliability, availability or safety. For example, the calculation of importance measures is a relevant outcome of the Probabilistic Risk Assessment (PRA) of nuclear power plants which allows evaluating the relevance of components (or more generally, events) with respect to their impact on the risk measure of interest, usually the Core Damage Frequency (CDF) or the Large Early Release Frequency (LERF). In other system engineering applications, such as aerospace and transportation, the impact of components is considered on the system unreliability or, for renewal systems such as the

manufacturing production and power generation ones, on the system unavailability. Information about the importance of the components constituting a system, with respect to its safety and availability, is of great practical aid to system designers and managers. Indeed, the identification of which components mostly determine the overall system behavior allows one to trace system bottlenecks and provides guidelines for effective actions of system improvement.

Chapter 7 provides some basic notions related to sensitivity and uncertainty analysis, in support to the analysis of the reliability and risk of complex systems under incomplete knowledge of their behavior. Indeed, as mentioned at the beginning, uncertainty is an unavoidable component affecting the behavior of systems and more so with respect to their failure limits. Thus, uncertainties arise in the values of the parameters and in the hypotheses on the structure of the models used to represent the system failure behavior. Such uncertainties propagate within the model used to compute the system reliability and risk, which become uncertain themselves. In spite of how much dedicated effort is put into improving the understanding of systems, components and processes through the collection of representative data, the appropriate characterization, representation, propagation and interpretation of uncertainty will remain a fundamental element of the reliability and risk analyses of any complex system. With respect to uncertainty, the final objective of reliability analysis and risk assessment is to produce insights in the analysis outcomes which can be meaningfully used by the decision makers. This entails that a number of topics be successfully addressed [12]:

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

In general, uncertainty can be considered essentially of two different types: randomness due to inherent variability in the system (i.e., in the population of outcomes of its stochastic process of behavior) and imprecision due to lack of knowledge and information on the system. The former type of uncertainty is often referred to as objective, aleatory, stochastic whereas the latter is often referred to as subjective, epistemic, state-of-knowledge [12,13]. Whereas epistemic uncertainty can be reduced by acquiring knowledge and information on the system, the aleatory uncertainty cannot and for this reason it is sometimes called irreducible uncertainty.

The distinction between aleatory and epistemic uncertainty plays a particularly important role in the risk assessment framework applied to complex engineered systems such as nuclear power plants. In the context of risk analysis, the aleatory uncertainty is related to the occurrence of the events which define the various possible accident scenarios whereas epistemic uncertainty arises from a lack of knowledge of fixed but poorly known parameter values entering the evaluation of the probabilities and consequences of the accident scenarios [12].

With respect to the treatment of uncertainty, in the current reliability analysis and risk assessment practice both types of uncertainties are represented by means of probability distributions [6]. Alternative representations based on different notions of uncertainty are being used and advocated in the context of reliability and risk analyses [12,14-16], questioning whether uncertainty can be represented by a single probability or whether imprecise (interval) probabilities are needed for providing a more general representation of uncertainty [17- 20]. It has also been questioned whether probability is limited to special cases of uncertainty regarding binary and precisely defined events only. Suggested alternatives for addressing these cases include fuzzy probability [21-23] and the concept of possibility [24-26]. Furthermore, probabilities have been criticised for not reflecting properly the weight of the evidence they are based on, as is done in evidence theory [27].

The issue of which framework is best suited for representing the different sources of uncertainty is still controversial and worth of further discussion. In the Chapter, the discussion is limited to the probabilistic representation of uncertainty, which is currently the most widely used in

practice. A recent critical review of the alternative frameworks of representation of uncertainty is provided in [28], from the starting point of view that a full mathematical representation of uncertainty needs to comprise, amongst other features, clear interpretations of the underlying primitive terms, notions and concepts. The review shows that these interpretations can be formulated with varying degrees of simplicity and precision.

From the point of view of the contents of the book, most of the material used to illustrate and address the above computational methods and issues has been drawn from the specialized literature on the reliability and risk analyses of complex systems. The specific contents are limited to a number of relevant topics and techniques which, in spite of not being exhaustive of the very extensive subject of reliability and risk analyses, can form the background material for a senior undergraduate or graduate university course on the subject or as basis for the initiation of young researchers to the field. To this aim, several numerical examples have been provided in support to the theory.

Finally, the realization of the book would have not been possible without the support of several people. In particular, I would like to thank Professors George Apostolakis (Massachusetts Institute of Technology), Marzio Marseguerra (Politecnico di Milano) and Drs. Luca Podofillini (Paul Scherrer Institute) and Andrea Zoia (Politecnico di Milano) for their contributions to the development of the Chapters {7}, {2, 4}, {1, 4, 6}, {3} and the examples therein, respectively. Many thanks are also due to Dr. Giulio Gola (Halden Reactor Project) for the initial translation of the Italian lecture notes at the basis of the material of Chapter 7 (it would have been too 'risky' to leave them as such). My last words of acknowledgments go to Francesco Di Maio who is currently pursuing a PhD at the Politecnico di Milano under my supervision: to him goes my deepest gratitude for the careful, precise work and for the unbreaking passion he has put into the editing of the book (perhaps motivated by the suffering he had to go through when studying the subject on the original lecture notes for my course).

Enrico Zio
Milano, July 2008

References

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

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

[3] Garrick, B.J. and Gekler, W.C., *Reliability Analysis of Nuclear Power Plant Protective Systems*, US Atomic Energy Commission, HN-190, 1967.

[4] WASH-1400, *Reactor Safety Study*, US Nuclear Regulatory Commission 1975.

[5] NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, 2002.

[6] Aven, T., *Foundations of Risk Analysis*, Wiley, 2003.

[7] Bedford, T. and Cooke, R., *Probabilistic Risk Analysis*, Cambridge University Press, 2001.

[8] Henley, E.J. and Kumamoto, H., *Probabilistic Risk Assessment*, NY, IEEE Press, 1992.

[9] Kaplan, S. and Garrick, B. J., *Risk Analysis*, 1, p. 1-11, 1984.

[10] McCormick, N.J., *Reliability and Risk Analysis*, New York, Academic Press, 1981.

[11] NUREG/CR-2300, *PRA Procedures Guide*, Vols. 1&2, January 1983.

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

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

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

[15] Da Ruan, Kacprzyk J. and Fedrizzi M. Eds., *Soft Computing for Risk Evaluation and Management*, Physica-Verlag, 2001.

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

[17] Moore R.E., *Methods and Applications of Interval Analysis*, Philapdelphia, PA: SIAM, 1979.

[18] Coolen, F.P.A., *On the Use of Imprecise Probabilities in Reliability*, Quality and Reliability Engineering International, 2004, 20, pp. 193-202.

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

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

[21] Zadeh, L.A., *Probability Measures of Fuzzy Events*, Journal of Mathematical Analysis and Applications, 23, 1968, pp. 421-427.

[22] Klir G.J., Yuan B., *Fuzzy Sets and Fuzzy Logic: Theory and Applications*, Prentice Hall, 1995.

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

[24] Zadeh L.A., *Fuzzy Sets*, Information and Control, Vol. 8, 1965, pp. 338-353.

[25] Unwin, S.D., *A fuzzy Set Theoretic Foundation For Vagueness in Uncertainty Analysis*, Risk Analysis 6(1), 1986, pp. 27-34.

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

[27] Shafer G., *A Mathematical Theory of Evidence*, Princeton, NJ: Princeton University Press, 1976.

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