Maîtrise des risques, sûreté et sûreté de fonctionnement : un regard sur la période 1990 à 2015, quel futur ?

Risk management, safety and dependability: looking back from 1990 to 2015, which future?

André Lannoy[1]

[1] Institut pour la Maîtrise des Risques, France, andre.lannoy@imdr.eu

RÉSUMÉ. Après avoir rappelé les principaux enjeux industriels, l'article montre l'évolution des démarches et des méthodes de la maîtrise des risques, de la sûreté de fonctionnement et de la sûreté de 1990 à 2015. Trois périodes sont mises en évidence. La première est orientée vers les préoccupations de la maintenance. La seconde, étant donné la rareté des ressources financières, s'intéresse à la maîtrise du vieillissement et à la gestion du cycle de vie. Enfin, la troisième, à la suite des catastrophes des années 2000, est une période d'aversion au risque et d'un retour vers les objectifs de sûreté. L'article explique ensuite comment est traitée l'incertitude durant cette période de 25 ans : modéliser et propager l'incertitude, gérer et analyser les données incertaines, décider dans un contexte incertain. L'article conclut sur les différentes actions qu'il conviendrait de mettre en œuvre dans un futur proche.

ABSTRACT. After recalling the major industrial challenges, the article discusses the evolution of approaches and methods of risk management, dependability and safety from 1990 to 2015. Three periods can be distinguished. The first is oriented maintenance purposes. The second, given the scarcity of financial resources, is concerned with ageing management and life cycle management. Finally, the third, after the disasters of the 2000s, is a period of risk aversion and return to safety concerns. The article then explains how uncertainty is treated during these 25 years: model and propagate uncertainty, manage and analyze the uncertain data, decide in an uncertain context. The article concludes with the different actions that should be involved in the near future.

MOTS-CLÉS. Maîtrise des risques, sûreté, sûreté de fonctionnement, incertitude, expérience, données du retour d'expérience, évolution des méthodes, futur proche.

KEYWORDS. Risk management, safety, dependability, uncertainty, experience, feedback data, evolution of methods, near future.

1. Foreword

Risk management and dependability appeared in Antiquity. Their foundations are based on mathematical methods set out in the seventeenth and eighteenth centuries. The first industrial applications mainly date from the 1940-1950 years. This article focuses on the years 1990 to 2015 and gives the vision of the author, after his experience in the nuclear sector, but also acquired from his European and French colleagues from other industries or universities within ESReDA (European Safety, Reliability & Data Association) and IMdR (Institut pour la Maîtrise des Risques, French institute for risk management, safety and dependability). Several topics are discussed in this survey, of course not exhaustive and partial as focused on the author's work issues.

The paper performs a critical review of progress in system reliability and safety, risk assessment, maintenance optimization, life time management, data acquisition and treatment, asset management, help for decision making, … During the period 1990 to 2015 the world has moved and changed with growing complexity trends. The paper tries to identify what has been tested and used, what developments are still needed and what new challenges are. Understanding the past prepares the future.

It should be noted that following the λμ16 Conference of Avignon in 2008, a prospective study on risk management in 2020 was conducted under IMdR [KAH 10]. The λμ Conference is the Francophone conference, devoted to risk management, safety and dependability, organized every two years by the IMdR.

Paragraph 2 discusses the evolution of industrial stakes during the period 1990 to 2015; three main periods can be distinguished for this evolution. Paragraph 3 recalls first of all that the study of risk is ultimately the engineering of uncertainty. Study of risk necessitates modeling and propagating uncertainty (paragraph 4), collecting, validating, analyzing uncertain input data (paragraph 5), deciding in an uncertain context (paragraph 6). Paragraph 7 focuses on the current conclusions and R&D prospects for risk management.

2. Industrial stakes and probabilistic analysis

2.1. *Industrial stakes*

In the early 1990s, industrial stakes were: 1 safety, 2 availability and performance, 3 maintenance costs. Environmental concerns, both internal (radioactive elements, borated water, corrosive fluids,...) or external (biodiversity, earthquake, ...), become more manifest around 1997-1998, the environment being both an aggressor or a receiver which has to be protected. Prioritization of stakes has consequently changed in the early 2000s: 1 safety, 2 protection of the environment, 3 availability and performance, 4 maintenance costs.

It is clear that the industrial objectives are to design, operate and maintain an industrial facility and its equipment in a **safe, reliable, robust, durable** (in the sense of ageing management and life extension)**, sustainable,** (and recently) **antifragile** way [TAL 13].

In engineering, robust design is a design that determines the nominal parameters of a product or system such that performance is sufficiently insensitive to any uncertain event that may encounter throughout the life cycle [LEM 14].

Antifragility is defined as a response to a stressor or a source of harm leading to a positive sensitivity to increase in volatility (or variability, dispersion of results, lack of knowledge, time, or uncertainty…, what is grouped under the designation of “disorder family”) [TAL 13]. This concept of antifragility is well expressed in economics. Antifragility is beyond robustness and resilience, the antifragility gets better and improves. It appears in risk engineering when lifetime management needs technical and economical methods and tools for managing ageing and optimizing preventive maintenance (paragraphs 4.3 and 4.4).

2.2. *Probabilistic approach*

The manufacturer and the operator must demonstrate the safety by the Probabilistic Safety Assessment (PSA, see paragraph 6.1) in which they must answer the following questions [BED 01]:

i. What can happen?

ii. How likely is it to happen?

iii. Given that it occurs, what are the consequences?

The nuclear, chemical, oil & gas industries have much invested in such evaluations including three levels:

Level 1: system analysis: it includes mainly event tree, fault tree, human reliability impact, feedback data bases, accident sequence quantification, uncertainty analysis; in the oil & gas sector Markov approach and Petri nets are also used;

Level 2: containment analysis: it includes characteristics of the release;

Level 3: consequence analysis: it includes analysis of the dispersion, toxicological effects, long term impacts, economic effects,…

Some specific PSA have also been carried out like PSA fire, PSA earthquake, PSA flood… The first PSA published, the Wash-1400 report [USNRC 75], concerned the BWR Peach Bottom 2 and PWR Surry 1 nuclear power plants.

2.3. *The main periods in the development of risk management*

Observing industrial concerns, several periods in the development of risk management, dependability and safety, can be distinguished between 1990 and 2015:

– *A first period 1990-1997* approximately, where research and applications are mainly *oriented maintenance issues*: development of the RCM (Reliability-Centered Maintenance) process, application to systems important to safety and production, integration of maintenance from the design, structuring operation feedback data bases for maintenance issues and maintainability, optimization of logistics support; "still as good or better and still cheaper", is the slogan of the managers of that era,

– *A second period turned to the "life cycle management"* (LCM) from 1997 to 2007-2008; investments are scarce, companies are concerned about ageing management, extension of service life, depreciation of their industrial assets; this is the period when we are interested in analyzing the degradation process (not only that engendered by a physical phenomenon but also the degradation of human behavior, of organization), in estimating structural integrity and safety, in extending lifetime with safety issues; it is also the arrival of the first industrial risk informed asset management process; the transition to the year 2000 proved to be a successful use of the methods of risk management and dependability.

– *A third period from 2007-2008 to 2015* (and not completed); this period begins with a sudden awareness, after the collapse of Minneapolis bridge in August 2007 which shows that the management of the lifetime of ageing structures and the lack of financial resources will become major problems for the future, especially when occur in the world very serious natural and technological disasters and several terrorist attacks (the 11th of September in 2001, 2004 tsunami, the sub-prime crisis in 2008, earthquake in Haiti, Deep Water Horizon and Xynthia in 2010, Fukushima in 2011, Lac-Megantic in 2013, Germanwings and Tianjin in 2015…). It's a *return to the safety objective* but not with the same spirit. It is no more than demonstrate safety as in the 1980s, it is now to maintain and especially to improve (at least a decade) safety or eliminate risk activities. It's the return of fears, risk aversion. The general public wants more security, more protection, and becomes much more demanding vis-à-vis industries, safety authorities, politicians. A distinction is made more and more between security and safety. Security is interested in events generated by intentional nature actions with a desire to harm. Safety seems to be more concerned with controlling risks associated with the design and the operation maintenance of facilities or equipment. Main advanced studies concern: the analysis of accident experience feedback, analysis of the direct and underlying causes of accidents, human and organizational factors, weak signals, safety indicators, but also the big data, health management, diagnosis and prognosis, the probability of rare events, risk analysis, physics- reliability modeling, estimation of consequences, crisis management.

3. Uncertainty

Recall that the ISO 31000: 2009 standard defines risk as the "effect of uncertainty on objectives". The uncertainty disappears when we are certain. In engineering, certainty is derived from observation or experience. The uncertainty is evaluated from the experience and measured by a probability. Very few books are available in the technical documentation on this important topic. In the international literature, we have identified the work [DER 08] published by Wiley and the recently published book [LEM 14], more oriented to the physics–reliability models, in particular mechanics- reliability models. Both books are outstanding works.

The uncertainty is related to the future: we try to measure it. It is often difficult to evaluate an uncertainty, due to lack of reliable and representative historical data, and to define the probability of

occurrence of a future event feared. It is also difficult to assess because the environmental - operating - maintenance conditions are also difficult to predict.

The probability of occurrence will measure the chance of occurrence of a feared event, either a relative frequency based on observation and interpretation of the historical experience or a probability based on knowledge, including experience and expertise (judgment / knowledge based probability).

Uncertainty has four components:

1- the inherent natural variability of a magnitude, irreducible character, or *aleatory uncertainty:* in time (variability of temperature ...), in space (variability of the rupture strength,...), due to the measure (performance of measuring means, ...); aleatory uncertainty can be quantified by measurements or statistical observation or by expert opinion;

2- lack of knowledge, or the *epistemic uncertainty*, reducible by increasing knowledge on the nature of the distribution (which is a subjective choice depending on sample size,…), on the nature of the model (insufficient physical understanding, uncertainty propagation, ...); the epistemic uncertainty shows how much could still be controlled if needed [BED 01];

3- *ambiguity* (it can be removed by well adapted definitions, information, …); ambiguity expresses the (legitimate) variability of estimates and interpretations relating to the observation of data or of identical facts or experiences;

4- *indetermination* (case of the extreme events, with very small probabilities and extreme consequences, in the Extremistan domain, see paragraph 6.1 [TAL 10]).

According to Der Kiureghian, Ditlevsen [DERK 09], the separation between aleatory and epistemic uncertainties is a matter of point of view. Indeed the distinction could be considered as a practical significance.

The two first components are the most common, the first one being often taken into account in many areas. The latter two components are often "forgotten" in the analysis.

Reduce uncertainty lies in analyzing, validating, processing and interpreting all the data observed from the experience (operation feedback, expertise, physical testing, knowledge data bases).

Risk can be considered as the engineering of uncertainty.

4. Modeling uncertainty and propagating it

4.1. *Dependability methods, system analysis at the design phase*

The dependability methods used in 1990 are the existing methods conventionally used: functional analysis, FMECA (Failure Mode, Effects and Criticality Analysis, always used in 2015 as an essential tool, both in design than operation), the event tree, the fault tree, the HAZOP method (HAZard and OPerability studies, mainly used in the chemical industry and in the oil & gas sector, and which deserves further use). At that time, the Francophone literature is fortunate to have a synthesis work on those methods [VIL 88]. The book of Cocozza [COC 97] should also be mentioned for his interest upon mathematical methods and tools and predictive evaluation of system reliability. All these methods can be implemented in the frame of design.

Regarding the fault tree, a very important contribution has been the use of BDD (Binary Decision Diagrams) in the Aralia solver which facilitates and accelerates the calculations while obtaining accurate results [RAU 97]. The GRIF module Tree software implements this algorithm.

The bow tie method, appeared in the 1990s after the Piper Alpha disaster, represents graphically results of risk analysis: the causes of the top event, the potential consequences, safety barriers in place

(paragraph 6.1). This very practical method expanded and is now used in all sectors, due to its graphical representation facilitating understanding.

Markov chains list the states (in operation, degraded, failed) of a system and the links between them. They provide a probabilistic assessment of reliability or availability, and identify weaknesses in a system. They assume constant dependability parameters (exponential hypothesis which does not always correspond to the fact in real world systems). If the system is a large scale system or a complex system (which is the case of industrial systems), there could be a risk of combinatorial explosion by multiplying the number of states, which can be avoided by modeling small individual Markov processes providing fault/ operation logic. The coupling between different methods (eg Markov / fault tree) makes it possible to develop powerful tools. Continuous time Markov processes are used by engineers to describe system dependability in many studies (implemented in the GRIF Markov module). A standard has been enacted in 2006 [IEC-61165: 2006].

Some studies are now performed in the field of dynamic reliability since the early 2000s [DUF 02]. The PDMP process (Piecewise Deterministic Markov Process [DAV 84]) is a process whose behavior is governed by random jumps at time points, where evolution is deterministically governed between those times [COS 10]. This process is little used in the industry. Yet the literature indicates that it would be possible to implement it while being able to take into account the variability of the data.

An important contribution, that still seems too little used also is the possibility offered by BDMPs (Boolean logic Driven Markov Processes). They are able to model real industrial systems [BOU 08]. They allow for studies of safety and availability of dynamic complex systems. The BDMPs are an alternative to fault trees and event trees. Their representation is graphical. The construction of the model is facilitated and it is possible to process very large sizes.

Used since 1983s, Petri nets are another dependability model whose use is increasing since the early 2000s. A Petri net consists mainly of places modeling the potential states (in operation, degraded, failed) of system components and of transitions modeling the events which can occur. Thus we can say that the Petri net encodes in compact form the set of states of the studied system and the transition that pass from one to the other. This method was originally used in automatic, dating from 1962. Calculations are performed using the Monte Carlo simulation. Applications concern reliability and availability of systems, repairable or not, probability of time spent in every state [SIG 14]. Despite some difficulties of the method (need to know it well, need of a lot of information: maintenance strategy, reliability laws of components, logistics, ..., difficult control and validation in the case of a complex system), the method seems booming. A standard has been enacted [EN 62551: 2012]. The GRIF Petri module software tool implements the method.

These Markov and Petri models experience since the early 2000s the competition of Bayesian networks, graphics, easier to implement and taking into account an uncertain context (paragraph 4.5).

Systems designed by industry are more and more complex. There is a double challenge of integrating the different engineering disciplines and the models they produce. This integration is supported by methods and tools. At the present time Model-Based Risk and Safety Assessment are developing [BAT 16]. This approach generalizes classical methods such as block diagram, Markov chains, …

In the mid 1990s, design methods evolve strongly. They not only integrate objectives studies, functional analysis, allocations and availability methods. They integrate more and more lessons from operation feedback and maintenance programs. They define the associated logistics support, the stake being to improve availability and industrial performance of production. In the 2000s, the design relies increasingly on reliability and technical-economic optimization. Durability (ability to perform a required function under given conditions of use and maintenance until a limiting state is reached) and sustainability become also important stakes. In the 2010s the robust design which is the resilience to uncertain events, becomes the main concern.

To demonstrate dependability of an innovative product or process, to develop methods for taking into account organizational and human factors in the design phase, to develop dynamic reliability models and management models of complex socio-technical systems, to evaluate the impact of a product or a facility on environment or health, seem to be the main priorities for the future.

4.2. *Structural reliability*

Stresses – resistance method is the basis of structural reliability. It is considered that there is failure when resistance is lower than stresses. These methods are not new [LIG 74]. They were already in use in 1990, in many industries, with Gaussian assumptions of stresses and resistance distributions. The stresses – resistance method may be applied to a system (a complex system), to a structure or to a single component.

Several books referring structural reliability were published in the period 1990-2015. Examples include: [MAD 86, DIT 96, LEM 05].

The behavior of a mechanical system may be characterized by a number of uncertain variables, random or deterministic, which describe the physical conditions or the environment: material properties, stress fields, geometric properties, possible existence of defects, and that may change over time as in the case of ageing.

Failures of structures are rare. Failure probabilities of structures are very low fortunately. Initially, the Monte Carlo simulation method was used to calculate these low probabilities (and is still used). However, it requires a large number of simulations to obtain an acceptable accuracy. Other methods may be used like first order-second order moment methods (hereunder), importance sampling, …

The concept of reliability index (mainly index of Hasofer-Lind [HAS 74]) is commonly used for characterizing the probability of failure or simply comparing the reliability of different structures. The input space of the random variables of the mechanical model (the physical space) is transformed to a space of independent centered-reduced Gaussian variables (by the transformation of Rosenblatt or other approximations). In this transformed space, the reliability index is defined as the distance from the origin to the point of the limit state surface the closest to the origin, point called the design point (according to the designer point-of-view) or the most likely failure point (according to the reliability engineer point-of-view). The FORM method (First Order Reliability Method) (and SORM, Second Order Reliability Method, which is a second order representation) provides an approximation of the probability of failure. The failure surface approximately coincides (first order approximation) with the hyperplane tangent to the design point. The FORM method is simple, not expensive in computing time, and solves 90% of real industrial case studies. It is nevertheless necessary to validate retrospectively the results.

The process of structural reliability has four main steps [DER 08]:

– the deterministic physical modeling (using analytical modeling, finite element modeling, ...),

– the quantification of uncertainties: existing data are processed statistically, they will be used to develop the probabilistic model,

– propagation of uncertainties: the aim is to estimate the failure probability with respect to design criterion,

– the prioritization of uncertainties to identify the most influential parameters.

Sensitivity analysis and assessment of margins are essential tools to highlight the most influent parameters and to judge the robustness. The physical understanding remains an essential condition of the quality of results. The engineer must always remember the proper physical sense in the interpretation of results.

The structural reliability methods are now operational. Software packages are available, for example open source software like DAKOTA, FERUM, OpenTURNS…

As against the processing of uncertain data remains a problem. Different methods are used to determine the probability distribution of a variable of interest: parameter estimation (which should not obscure the physical consistency), non parametric estimation (underutilized, which has the advantage of considering only the available data and of not applying a prior model), the polynomial chaos (or Wiener expansion chaos [LEM 14]) which is is a non-sampling-based method to determine evolution of uncertainty in a dynamical system, or possibilistic models [GAO 96, SAL 06].

Also are emerging new methods, applied to structural reliability, such as Support Vector Machines (SVM) [LI 06] whose principle is to seek the separation between the positive and negative values of the failure equation (the performance function), and Kriging which is a Gaussian process regression method of interpolation for which the interpolated values are governed by a Gaussian process [DUB 11].

The first applications of these methods in reliability date from the 2000s. To date it is found that the methods of structural reliability rose sharply over the 25 years. Yet they are still too little used, for various reasons: they are considered complex by industry, the tools are considered not suitable, they require difficult access to relevant data, which are difficult to treat and analyze. But today performing tools exist, it remains to educate and to train the engineers.

Many ESReDA project groups have been focused on industrial applications of structural reliability. They include [THO 98, DEL to be published], [LAN 04] on the lifetime management of facilities, [ARD 10] on the place of the Structural Reliability Analysis (SRA) into System Risk Assessments (SRA), and soon another ESReDA book on optimizing the reliability and cost of the life cycle [CHA to be published in 2017].

The priority areas to develop in the future appear to be the processing of input data and the theme of reliability and robustness. Writing a practical guide would be certainly useful. Time variant reliability problems may have also an interest for the future. It appears in engineering when the deterioration of material properties with time and random loading modeled as random process are involved. The paper [AND 04] presents an application on a mechanical system in an exceptional configuration and compares to other methods.

4.3. *Maintenance modeling*

By 1965 Barlow and Proshan [BAR 65] showed the impact of maintenance on reliability.

Equipment may be reliable if it is well designed and if well maintained.

Maintenance was a constant concern of industry during this period of 25 years, for many reasons [PET 01, AND 10]:

– maintenance costs have to be reduced,

– safety / security goals have to be maintained and even improved; maintenance is indeed often involved, especially in transport, as a direct cause of major accidents,

– maintenance becomes important at the design phase [BOUR 98], now equipment and services (operation - maintenance) are bought; industrial performance, in particular the availability and the quality of service but also preventive maintenance and logistics associated support have to be optimized from the design phase [RAZ 14],

– durability (ageing management and life time extension) and sustainable development have become major issues because of the scarcity of financial resources and environmental protection will.

– The RCM (Reliability Centered Maintenance) methodology appeared in Europe in the late 1980s and has been deployed in industrial systems in the early 1990s. Objectives were:

- maintain and improve safety objectives of industrial sites,

- reduce unavailability (scheduled or shutdown),

- lower the maintenance costs,
- optimize maintenance interventions (in frequency, duration, for the grouping of maintenance actions ...).

Preventive maintenance, less expensive than corrective maintenance, prevents failure and downtime, so to be safer. The RCM approach is applied to large systems, primarily those important to safety and then those important to production. The results are almost immediate: better reliability of equipment, improvement of the collection of feedback, 10 to 30% reduction of maintenance costs.

The context (the environment, operating conditions, maintenance) are constantly evolving. RCM approaches are periodically updated, every 3 years for important to safety systems, every 5 years for the important to availability systems.

A large number of standards, military standards and recommendations have been published in the period (including in particular MIL-STD-2173 or SAE JA 1000 [SAE 12]).

In the late 1990s, condition monitoring becomes more systematic: it wants to monitor the most critical equipment and allow at earlier its repair or replacement. Monitoring data and inspection data are recorded to establish a behavior assessment check-up of critical equipment [DEH 04]. Specially interesting are degradations, their mechanisms and their kinetics: physical laws, regression models, Wiener process and especially the gamma process are the models the most used for processing inspection data [SIN 97; NIK 02]. In this period of the late 1990s – early 2000s, this objective of estimating laws of degradation kinetics proved difficult given the number of degradation mechanisms to examine and the insufficient number of degradation data available. The probability of detection of a defect and the reliability of NDT (Non Destructive Testing) become important subjects upon which maintenance decisions strongly depend.

Operation feedback analysis, operating conditions recording, analysis of monitoring data are used to establish a diagnosis (or a health status) of equipment at the time of observation. From this review it is hoped to predict the future behavior of equipment. It provides strategic maintenance alternatives which are then defined, explored, evaluated. It is called predictive maintenance (sometimes called exceptional maintenance in some industrial sectors or physical asset management, performed through all the life cycle phases) which is a condition based maintenance carried out following a forecast derived from the analysis and evaluation of the significant parameters of the degradation). Predictive maintenance becomes a priority in the late 1990s.

Maintenance decision ultimately will depend on:

– the health status of the equipment,

– its predicted physical behavior and its predicted reliability,

– economic criteria (often the NPV (Net Present Value) is optimized using industrial asset management models),

– sustainable development: in particular, that is the question of extending the lifetime of plants and components, avoiding damage to the environment.

Reliability proves to be the overriding factor in the decision, leading engineers to examine the effectiveness of maintenance on reliability, until the early 2010s [DOY 11; PRO 11].

The AP-913 approach [INPO 01], imported from the United States in 2007, has been installed in some industries. It seeks continuous improvement in reliability, anticipation of problems, the permanent adaptation of maintenance programs, the organization of maintenance in industrial sites.

The EN 13306 standard on the terminology of maintenance has been published (1st edition in 2001, 2nd edition in 2010). This standard is very useful not only for maintenance purposes but mainly for reliability and dependability studies.

Systems are increasingly complex. It becomes more and more difficult to determine the precise origin of a failure. Solutions of significant improvement of the diagnosis function must be sought. Another progress axis concerns the improvement of system availability, anticipating maintenance tasks in advance before failure. This goal involves the failure prediction function, thus reducing maintenance costs by performing the maintenance task just before needed time. These topics come back today in 2015, although some industries (air-space and nuclear sectors) are already heavily involved. HUMS systems (Health and Usage Monitoring System) [IMdR 15] are implemented to monitor and record the physical and electrical parameters of equipment and facilities, and realize the different treatments of the data recorded (using data analysis, text mining, big data packages) to pinpoint failures (by an extended diagnosis) and thus anticipate potential remaining lifetime before failure (prognosis). This is to further improve the failure diagnosis and prognosis.

4.4. *Ageing management*

Ageing is the general process in which characteristics of an SSC (System- Structure- Component) gradually change with time or use [EPRI 93]. Attention to ageing appears in the years 1995-2000, almost the same time than sustainable development objectives. Financial resources become scarcer. If degradation mechanisms are well controlled, the economic interest of extending the lifetime of a plant and its equipment is obvious, especially for heavy installations, requiring large investments. It is essential to identify the main vectors of ageing, to detect, assess and prioritize them, to take the necessary measures to mitigate, defer or delete them.

The lifetime is unfortunately a post mortem concept. We only know the lifetime when an unrecoverable major fault occurred. This case is rarely found in practice since it seeks to avoid this situation and that generally the technical - economic optimization decides the lifetime. Lifetime can also be the result of a planned obsolescence.

The table 4.4 presents the main trends in ageing studies [IAEA 02; LAN 05].

Numerous studies have thus been developed:

– detection of ageing by Bayesian techniques [CLA 04]; another method, non parametric, the TTT (Total Time on Test) method seems little used, although it can detect unfavorable behavior of a component, repairable or not, and assess an approximate value of the time of initiation of a possible sad evolution; it can be recommended due to its simplicity, its readability and the fact that it takes into account the uncertainty of field data, completed or right-censored (regardless of model) [KLE 82];

– analysis of degradations, especially their kinetics; we are interested in different physical mechanisms and seeking to determine a law of degradation in the service context, using physical models (for instance, using Time Limited Aging Analysis (TLAA), accounting situations and transients in the case of thermal fatigue), or using regression methods or the Wiener process or especially the gamma process to analyze inspection data or monitoring data (paragraph 4.3); these degradation laws may determine a residual life (or remaining life: actual period from a stated time to retirement of an SSC) and permit to optimize preventive maintenance,

– when the status of the most critical and most expensive components is diagnosed, their future behavior can be anticipated [BOUZ 05; PET 06]; for this purpose one determines the durability after updating the operating conditions; possible options are identified (corrective maintenance, the optimized or more aggressive preventive maintenance, refurbishment, or replacement or new design), which are evaluated as a reliability-economic point of view; diagnosis and prognosis still remains a field in progress (see HUMS systems, paragraph 4.3),

– equipment behavior can then be prepared and foreseen, indicating the efficiency of maintenance operations; the manager can decide between options from do nothing, optimized preventive maintenance, … to predictive maintenance, which is called in some industrial sectors exceptional maintenance and which aims to exceptionally replace a large critical component by another new one or by a more efficient technology,

– inspection timing is important for life extension in allowing equipments to continue operation by exceeding their design life in the most economical manner; in that frame, RBI probabilistic methods (Risk Based Inspection) can provide very useful information,

– a LCM (Life Cycle Management) approach has therefore been developed from the 2000s, comprising technical and economic methods of Risk Informed Asset Management (RIAM) and investment optimization [SLI 03; LON 12].

Ageing databases (like the GALL report (Generic Aging Lessons Learnt; [USNRC 10]) do not exist in Europe, to our knowledge. It seems that this is an oversight and knowledge management tool that would be useful to industry. Nevertheless, data bases concerning ageing of material characteristics have been developed in the nuclear industry.

Objective	Safety	Availability / Performance / Production
Impact	On safety related functions	On availability, profitability
Phase 1: identification	Rather passive components Some active components	Rather active components Some passive components
Phase 2: evaluation	Degradation models Estimation of the residual lifetime	Reliability models Efficiency of maintenance
Phase 3: mitigation	Condition based maintenance	Preventive maintenance Predictive maintenance Risk Informed Asset Management (RIAM)
Domain	License Renewal	Life Cycle Management

Table 4.4. *Main trends of ageing studies (in the nuclear industry)*

4.5. *Influence diagrams and belief nets*

Several methods can be considered fit to represent and propagate uncertainties. Belief nets grew in the late 1980s to manage uncertainty in expert systems. They include: numerical simulation (used however from the late 1960s), fuzzy set theory (the Dempster-Shafer theory uses belief functions and plausible reasoning; its purpose is to compute the possibility of an event), Bayesian networks, belief networks, evidential networks (VBS, Valuation Based Systems).

VBS is a framework for knowledge representation and inference. Real-world problems are modeled by a network of interrelated entities, called variables. The relationships between variables (possibly uncertain or imprecise) are represented by the functions called valuations. An application to risk management is published in [BEN 09] and concerns decision-making in the military field. It is in this publication to provide a decision support by providing an analysis of threats estimated on the basis of probability of threats or of threats plausibility. The uncertainties are represented by belief functions.

Some references presented recently show their applicability to reliability, risk analysis and decision support. Article [BIC 08] concerns the modeling of safety instrumented systems design, based on reliability networks, to meet a SIL (Safety Integrity Level, [IEC 61508: 2010]), where optimization is performed by genetic algorithms. Article [AGU 13] in the rail sector takes into account the human reliability by using evidential networks and fault tree analysis.

These methods seem attractive for applications of risk management and risk analysis:

– they are supported by a graphic representation, which helps their reading and understanding,

– they seem well adapted to the context of uncertainty (including epistemic uncertainty),

– they can take into account the situations of ignorance,

– they generalize the methods commonly used by the engineer in risk management or dependability, such as fault tree or Bayesian network.

The Bayesian network [JEN 96] is now in 2015 widely used in risk management and dependability since the late 1990s. Industrial applications are numerous: diagnosis, prognosis, anticipation, law of degradation, risk analysis, analysis of emerging risks, proactive assessment, help for decision making, efficiency of actions [WEB 12]. Bayesian network is a directed acyclic graph to represent probabilistic variables, qualitative or quantitative. This graph is both:

– a knowledge representation tool, a knowledge management tool: the nodes are variables or groups of variables, arcs between nodes reflect the influences (is influenced by, influences; for instance [COR 06]),

– a probabilistic Bayesian inference which is based on the conditional probabilities,

– a decision support for introducing action variables and measuring the effectiveness of action.

The input data are often uncertain experience feedback data or expert judgment. Action nodes can be introduced: they represent the possible actions to a decision maker. The difficulty mainly lies in the construction of the network structure and its validation. The great advantages of the Bayesian network are their ability to take into account the uncertainty of variables and the graphics promoting reading and understanding. The output results are usually the identification of the most influent variables, critical paths, facilitating thus the choice of a decision and the assessment of its effectiveness.

Powerful software packages (for instance Bayesia in France or Netica in Denmark) are available.

The influence diagram is a graphical representation of a proposed decision. It is widely used (see paragraph 5.5). It can be an alternative to the decision tree (paragraph 6.2) difficult to manage when the branches are many. It is well suited to modeling problems of organizational and human factors.

Apart from the Bayesian network and the influence diagram, probabilistic networks still seem little used in risk management and dependability, although they seem appropriate to many needs. In this context, merging of heterogeneous data, fuzzy logic, possibilistic approaches to the provision of data have to be examined.

5. Collecting, validating and analyzing uncertain data

5.1. *Operation feedback: failures and degradations*

In 1990, the feedback is mainly directed towards safety. In different industrial sectors (especially nuclear and oil & gas) databases were structured. Their content is mainly used to provide reliability data required for safety assessments. Failure sheets, their quality, their accuracy and relevance, are validated in a first step [PET 99]. Failures are then analyzed. This failure analysis shows the usefulness of the description of the failure in the free text summary of sheets, to qualify, to complete or to classify information [LAN 94]. Failure rates, on demand failure probabilities, reliability laws, repair times, equipment unavailability times are estimated assuming an exponential reliability law or a Bernoulli distribution for equipment subject to demands [MOS 05]. All these processed data are regularly published in reliability data handbooks. The latest editions, to our knowledge, are the following:

– *Electronic components*: MIL-HDBK 217F (1991), RDF 2000 (2000), UTE C80810 (2000), 217Plus (2006), FIDES (2nd ed., 2009),

– *Mechanical, electrical, electromechanical components*: Tables AVCO (1963), CCPS (1989), NPRD-95 (1995), EIReDA'1998 [PRO 98], EIReDA'2000 (2000), T-Book (6th ed., 2005), NSWC-2006 (2006), ZEDB (2008), NPRD-2011 (2011), OREDA (6th ed., 2015).

We must remember that the values of these published handbooks are generally safety-related data. OREDA nevertheless is a general data basis collecting failure data and maintenance data, being consequently well adapted for safety and availability studies. At present, except perhaps in the

electronic field, efforts for publishing handbooks seem unfortunately become rare, probably given the difficult, tedious and costly nature of the analysis and the confidentiality of data. It turned out that the important data for safety are not sufficient for maintenance.

A new collection strategy and a new structure were therefore defined to address maintenance issues [LAN 94; SAN 03; ISO 14224: 2016]. In this new structure, fields have been added, especially the analysis of degradation or failure, specifying the different indenture levels (system, subsystem, component, spare part) of functional – equipment tree, failure mode, the degradation mechanism (or measurable effect), maintenance costs, specific free texts analyzing safety- maintenance- human factor aspects. These different fields and those needed for safety assessments provide the data needed to process PSA and RCM (paragraph 4.3).

Another issue is probably data capitalization in an ageing database required for lifetime studies and life extension. Such a base goes beyond the now classic bases for maintenance. It will also gather the knowledge acquired over the operation, potential degradation mechanisms, effects of these mechanisms, the associated degradation kinetics, the observed failures and right censored data (with a view to determining a survival law), operating and monitoring data (health and usage monitoring data).

As said before the future of feedback lies in free text analysis and interpretation. The experience feedback includes indeed an increasing amount of text descriptions. The textual tools can help to exploit faster operation feedback: searching for information, checking the quality of data, clustering, identification of similar events, case based reasoning, text mining... This theme is a great potential research subject.

Big data could be valuable tool to the analysis and expertise in their ability to process large volumes of data and to highlight facts that we do not suspect. Big data allows us a finer risk analysis. It is a proactive tool, minimizing the risk that an undesirable event occurs or better measuring the consequences. However big data necessitate large amounts of data, which is not obvious in risk studies where data are mainly rare. We have to be able to read and interpret big data results.

Knowledge management (KM) and a consideration of the context will improve the detection of weak signals (paragraph 5.3) and other relevant non technical factors that can improve the decision, while enhancing safety. At the design stage, a KM approach facilitates the construction of models for defining systems architecture and equipment, and accelerating the manufacture of equipment. In summary, an adapted approach of Knowledge Management will strengthen the innovative capacity of companies, make them more competitive, more sustainable and less vulnerable in the context of a global hyper-competition.

Finally, note that, to succeed, the feedback requires clear direction of management, training of people involved, good organization, user-friendly tools and guidance to users.

5.2. *Frequentist methods and Bayesian inference*

The objective is to determine a probabilistic law of behavior of a component or a structure, in short, to estimate the parameters of the component reliability law, also known survival law. The best reference is certainly the Meeker- Escobar book [MEE 98].

The field data, which always require validation within the meaning of the accuracy and relevance, treatment and analysis, has the following characteristics:

– .they are few, the sample size is small, components have very few failures due to their good design or an optimized preventive maintenance,

– .the sample is heavily right censored; indeed, feedback experience identifies very few failures and a high number of right censored data (truncated data type I), corresponding to good functioning or end of observation [BAC 98].

In the early 1990s, only the exponential distribution is used. Reliability data from most of the handbooks also assume an exponential distribution. Everything changes in the years 1995- 2000 when we begin to worry about optimizing preventive maintenance and ageing problems.

The Weibull analysis for non-repairable components becomes systematic. For repairable components failure intensity is modeled by a power law [PRO 11]. The problem is to estimate the parameters of the laws given the observed data. The most used method when the number of failures is high (> 20) is the maximum likelihood method. Estimators are the values that maximize the likelihood function.
When the number of failures and sample size are small (between 6 and 20 failures) other approaches that aim to provide more reliable estimators can be used [BAC 98]. A first approach, frequentist, uses a stochastic algorithm SEM (Stochastic Expectation Maximization), particularly in the case of very high censorship. The bootstrap technique (which is a statistical inference based on a succession of resampling, and which allows us a very fine sensitivity analysis), used first time in Europe in the 1990s, permits to determine the laws of distribution of parameters and to calculate the mean and standard deviation of these distributions. When the number of failures is even lower (< 6), the problem can be placed in a Bayesian framework to take into account a priori knowledge on these parameters, the knowledge coming from expertise or generic data or past data handbooks. The difficulty lies in the construction of this prior one hand and Bayesian inference (BRM algorithm, Bayesian Restoration Maximization) on the other.

The Bayesian inference has several interests [CLA 98; SIN 06]:

– .it proceeds from a learning process,

– .it determines the distribution laws of parameters, the posterior mean and the variance and therefore estimates the level of uncertainty that we have about the parameters,

– .it is able to take account of multiple forms of knowledge such as expert judgments, previous reliability data, a priori knowledge, enriching global knowledge and thus reducing uncertainty,

– .it is used to update data or to individualize the parameters: it can be noted that this principle of updating is now commonly used in PSA and are also in data handbooks (eg EIReDA'2000 and T-Book).

In order to approximate the posterior sought, one can use a MCMC algorithm (Monte Carlo Markov Chain), which is not always effective, or an IS (Importance Sampling) preferential sampling algorithm. It should focus on the estimation of the shape parameter of the laws because it reflects the kinetics of degradation of equipment.

These frequentist estimates have emerged in the 1990s and, as a result of things, Bayesian approaches have been developed in numerous industrial sectors. At present frequentist and Bayesian methods are complementarily used in dependability studies mainly to quantify a reliability law or uncertainty or to update parameters. Bayesian methods continue to develop, mainly on the subjects of maintenance efficiency or elicitation of expertise.

It should not forget the non-parametric methods, always interesting, because they are readable and contain only data uncertainty (there is not a subjective choice of a distribution). The Kaplan-Meier estimator [KAP 58] which has the property of maximizing the likelihood, the median ranks method of Johnson [JOH 64] are very practical methods but too little used.

5.3. *Operation feedback, accident analysis*

Similarly the event – incident – accident data were collected in databases of events well before 1990. These events are either important to safety events, or events with loss of production, or also events considered critical (whose origin can be for example an external natural event, an external event, the failure of a major component ...).

Important events (such as major accidents) are the subject of detailed analysis afterwards. Minor events are also analyzed and classified into families. These events also help to assess the performance of the industrial plant or of its components (including the availability, safety, the number of reported incidents, the number of accidents, different safety indicators...). In the 1990s, the analysis mainly concerned technical but also human aspects. In the late 1990s and beyond, industry was interested in environmental and organizational aspects, in order to learn how to limit the number and the severity of accidents.

In 2009, a very important report that refers throughout Europe is published by the project group "Accident Investigation" of ESReDA [ESReDA 09]. The ambition of this guidelines report is to reflect the state of the art in accident investigation as well to address its future challenges. This guidelines report gives a generic state of the art of principles, models, aims and methodologies for accident investigations. It describes the main elements of managing and conducting an accident investigation, in the aftermath of an event and focuses on how to learn from the results of the investigations when designing corrective and preventive actions and also looks at barriers to lessons learning.

The topic is important and is the subject of numerous researches that have to be carried on. There are still so many major accidents, progresses resulting from accidents seem limited. We do not feel that the lessons of the past are effectively acquired by industry.

The challenges are many:

– research the root causes, direct and underlying, of accidents, which leads to consider the organizational factors and the identification of the factors of robustness and resilience of organizations; AcciMap [RAS 97] is a systems based technique for posterior accident analysis, analyzing the root causes of accidents that occur in complex socio-technical systems; factors contributing to accidents can be analyzed and safety recommendations can be formulated; AcciMap seems attractive in the sense that it can serve as a basis for the construction and validation of a probabilistic network structure; TRIPOD is a method identifying organizational failures likely to have an impact on health and safety at work [CAM 08]; in France are also used cindynics methods (which do not seem used elsewhere in Europe) for the posterior analysis of industrial accidents; the cindynics methods can also be used at the design phase when it comes to highlight the human and organizational factors contributing to risk [KER 91; CON 06; BAI 13];

– anticipation and a priori detection of weak signals announcing more serious "unthinkable" events: the role of whistleblowers, weak signal detection by statistical methods (like data analysis, big data) or free text analysis (by text mining), contribution of probabilistic methods to expert analysis,

– methods for estimating the probability of rare events to extreme risks and the determination of distribution tails laws or the probability of zero failure [WEL 74; HIL 75; DEH 13; GERV 16]: indeed the risk lurks in the distribution tails,

– consequence modeling: when estimating the probability is difficult or when a plausible event is very unlikely, it becomes very important to consider the physical models to calculate the probability [MOR 15] and the consequences; these consequences are they acceptable? The estimate of the consequences is the first step, the first parade to protection from unpredictable events,

– finally the knowledge management about major accidents in different industries (which needs the creation of an international data basis of major events), to establish a prognosis on the future behavior of a system, an organizational diagnosis of safety, to question practices or improve event analyzes and more generally to improve the whole operation feedback system.

5.4. *Expert opinion*

The expertise has become a widely used source of knowledge since the mid-1990s [COO 91]. Expertise is authorized and informed opinion, based on experience. This is a possible answer to a technical problem, to "facilitate" the decision of a decision-maker. It allows to complete, to improve objective data when they exist and when they are few, questionable or not applicable, or to compensate

them when the data are missing (eg in the case of a bad feedback or a future problem or an innovation ...). This is often the only available source of information to assist a decision maker in his decision. It is a source of subjective information, representative of an opinion authorized and recognized but based on knowledge, training, practice and experience of experts in a particular area at a given time. It is a source of data that can be qualitative or quantitative.

The expertise is a source of prior information. It is essential when:

– .the feedback is rare or nonexistent,

– .the future is not the image of the past: new risks, new design, innovation, design modification, renewal, changes in environmental conditions, modifications in operating procedures or maintenance programs.

Expertise is uncertain. Several actors are involved in the expertise: the experts, the analyst (or facilitator or moderator), the decision maker. The main difficulty lies in the elicitation of expertise.

The problems of elicitation include [BOL 05]:

– .the choice of experts,

– .the elicitation, where one can distinguish various interrogation methods (individual interviews, interactive groups, Delphi method),

– .the analysis of expert answers (in consideration of bias, weighting and aggregation of expertise (calibrating)),

– .modeling of response and uncertainties, the expertise efforts and costs to consent to the collection, analysis and modeling expertise,

– .the knowledge management.

The European approach KEEJAM (Knowledge Engineering Expert Judgment Acquisition and Modeling) is well suited to expert elicitation [COJ 98]. It is based on knowledge engineering.

The Bayesian framework is well suited to modeling expertise data. It allows to take into account any expertise and any structured operation feedback. Sensitivity analyzes must always be performed. We find the use of expertise in many industrial applications: reliability, updating data of a reliability handbook, Weibull analysis, diagnosis and prognosis, maintenance optimization, ageing, estimating maintenance efficiency, help for decision making, risk analysis. Many industrial applications are presented in [LAN 01].

The tracks to be developed in a near future concern the development of a practical guide and associated tools to merge feedback and expertise, user guides of expertise throughout the life cycle, the use of expertise in diagnosis - prognosis, knowledge management approaches and tools.

5.5. *Human factor data*

The human factor contributes greatly to the failures of socio- technical systems and thus to major accidents. 374 accidents on the 604 accidents recorded in France in 2012 in the ARIA database, where 61.9% of accidents, are attributed to organizational and human factors. However, if man is the cause of many accidents, it is also a recovery factor to reduce or even negate the impact of accidents. The importance of human and organizational factors in the frequency and severity of accidents is now well recognized, which was not the case in the early 1990s.

The first human reliability studies have emerged in the Wash-1400 report [USNRC 75], where human error probabilities are used. Since then numerous studies have been carried out. Yet little quantitative data are currently available. When they exist, they are also often contested or considered irrelevant.

The best-known work [SWA 83] is the basic reference to all books and articles published after 1983. The methodology, called THERP (Technology For Human Error Rate Prediction) estimates the probability of human error (which can be defined as: human output that has the potential for degrading a system in same way) or of success. Man is regarded as one of the components of a system. These data were and are still used in Probabilistic Safety Assessment (PSA).

Thirty of human reliability analysis methods (whose origin is often the nuclear industry) have been identified since 1983 by [SOB 15] but, in truth, in practice, no of them is distinguished by its wide use in the industrial world. Early methods were named methods of first generation, they have focused on human error. In the early 1990s, other methods, known as second generation, appeared. They consider that the probability of failure also depends on other factors, "cognitive", as experience, training, adaptation, ageing ... One can quote for example:

– the CREAM methodology (Cognitive Reliability and Error Analysis method; [HOL 98]; a Fuzzy CREAM version has been developed by [MAR 07],

– the MERMOS methodology [BIE 98; LEB 10] developed from the end of 1990s; it is a reference method for Human Reliability Assessment to assess the emergency operation of nuclear reactors during incidents or accidents; the methodology is effectively used in PSA,

– the SPAR-H methodology, developed by the Idaho National Laboratory [GER 05], the failure probability distinguishes diagnosis failures and action failures.

Despite many years of work, there is no consensus. Perhaps this is due to systemic or too detailed orientation, and therefore too complex, preventing any progressive advance. It seems to go round in a circle. Human factor data is nevertheless essential.

Presumably probabilistic networks, which can take into account interactions and uncertainties can provide valuable assistance to the analyst [AGU 15]. These probabilistic methods have been used in the nuclear sector with uncertain variables, technical or behavior, qualitative or quantitative. It is clear that the man has to be modeled in its context and in its environment. The work of [EMB 92] seems very important but rarely used. Using an influence diagram, it is possible to model the human and organizational behavior that can lead to human error, taking into account cognitive factors and other causative factors of context. This idea was taken up by [CLA 94] for the analysis of a maintenance task and determination of its efficiency.

Probabilistic networks are currently used in the humanities, sociology and criminology [SCH 15]. For example, the Zürich police is testing the use of the software Precobs (Pre Crime Observation System) to predict the likely future locations of burglaries. Based on 5 years of police statistics, demographic data, data of social networks and some influential variables considered, the software determines the most likely places burglary with a success rate of 4/5.

One can nevertheless point out that the human factor is now taken into account in safety studies as in design, which was not necessarily the case in 1990. The progress has been consequently significant as said in [FOR 09], where it is argued that it has become important to understand and model the cognitive aspects of human performance and to list the factors that have been shown to influence human performance. It is concluded that Human Reliability Analysis is currently able to adequately predict human failure events in a complex domain and their likelihood.

6. Deciding in an uncertain context

6.1. *Risk analysis, safety, accepting risk*

Risk management is the process of analyzing exposure to risk, determining how to best handle such exposure and monitoring effectiveness of risk management efforts.

Methods aside, appears, after the Piper Alpha disaster (1988), in the early 1990s, the bow tie method that visually materializes accident scenarios that may occur, starting from the initial causes to the consequences. The bow tie method is now in common use in all industrial sectors.

The QRA method (Quantitative Risk Assessment) was used in the 1990s, even at the end of the 1970s. It also can be called semi-probabilistic method. It is still very widely used in the 2010s in all industrial sectors. The operating experience feedback databases are used to estimate rates of occurrence of failures or events and to describe accident scenarios whose consequences are then calculated by physical models.

The ARAMIS project (started on 2002; [HOU 14]) aims at developing a risk assessment methodology which allows to evaluate the risk level of an industrial plant by taking into account preventive measures against accidents and the vulnerability of the environment. The result is the composition of an integrated risk level based on the definition of reference scenarios and combining the evaluation of consequence severity, environment vulnerability and safety management effectiveness.

The first PSA, the Wash-1400 report, was published in 1975. The first European PSAs were carried out in the 1980s. PSA are designed to assess the annual frequency of destruction of barriers and the associated release of radioactive products. Since the 1990s, the models have changed little. Development efforts have focused on processing data including understanding the human factor, but also the updating of data required for PSA (critical failures, operating profile, initiating events, procedures, human factor data), the PSA being updated every 10 years, important to safety data being updated every 3 years. The safety authorities recommend living PSA to operators. We also note the establishment of safety indicators and monitoring of reliability characteristics of critical components by the analysis of feedback, the creation of safety data handbooks and writing of behavior assessments of equipment.

Efforts are also focused on software tools and, currently, the Swedish RiskSpectrum software is used in all European countries. As part of the European Open PSA project (2010), an input data format has been set to allow users to work with different software packages but with the same data format.

Specific PSA emerge in the 2000s: the PSA earthquake, PSA fire, PSA flood. The implementation of a seismic analysis in PSA consists in several steps: estimation of the frequency of exceeding specific peak ground acceleration, fragility estimation, internal initiating events analysis, modeling.

If the PSA were controversial in the years 1975 - 1985, they are now used despite their limitations in many industrial sectors, including the nuclear industry, process industries and civil engineering.

Limitations of probabilistic approaches are mainly due to:

– model uncertainty: there is no perfect model; physical knowledge, the level of detail and assumptions determine the accuracy of the model;

– data uncertainty: the use of expert data, problems of existence, collection and accessibility, quality (in the sense of the accuracy and relevance), feedback variability makes complex the use of data;

– the changing context: things can not be known with perfect certainty, because of their continual change.

Therefore, it is necessary to strike a compromise between the needs of decision support and efforts to implement for models and "refined" data. Note that PSA results must be examined in relative, the sensitivity analysis is consequently essential.

The first risk analysis dates from the late 1970s: Canvey Island in 1978, Rijmond in 1982. The UK and the Netherlands are pioneers, France only in 1983. Today the practice of risk analysis is common, at least in large process industries. In 2009, the ISO 31000 standard recommends the risk analysis approach. The recommended methods are deterministic and probabilistic. They cover different areas of

physics such as mechanics, heat transfer, fluid flows, detonics but also economic models and demographic models.

A big question that companies have to deal with is: “how safe is safe enough?” [FIS 78]. That can be restated as: what is the acceptable risk level?

Results of probabilistic studies are compared to the allocated targets or to acceptance criteria, usually probabilistic (for instance the Eurocode EN 1990: 2002). One can trace the curve of Farmer, fC (frequency - consequences) or FN (frequency - number of fatalities), leading to indetermination in very low probabilities. Or one can use the criticality matrix, often very approximate and subjective.

In 1992, the Health and Safety Executive in UK [HSE 92] proposed the ALARP approach (As Low As Reasonably Practicable). The ALARP principle presupposes that there is a tolerable level of risk and that risk should be at least below this level. The term "reasonably practicable" means that a risk considered low level may be transferred to an area where the risk becomes negligible. An infinite effort could reduce the risk to an infinitesimal level, but this effort would be infinitely expensive. This is why the ALARP method assumes that there is a level of risk as it is not worth the financial effort to reduce it again. This means that all preventive- protection measures should be taken until a risk reduction cannot be made without a significant increase in investment or expenditure. In other words, the expenditure would be disproportionate to the gain in achieved safety.

In the region "intolerable", it should reduce the risk and move to the region "tolerable if ALARP". In this region ALARP, it is recommended to make every effort to reduce the risk. The stop level of these efforts is the subject of an analysis, discussion and compromise. The region "broadly acceptable" includes all situations of very low probability; its level is an upper bound of the probability of a rare event "unpredictable".

Many European countries are practicing this method. By design the region “tolerable if ALARP" is for the public between 10^{-4}/ year (upper tolerability limit (fatalities per year)) and 10^{-6}/ year (lower tolerability limit) and respectively for the workers between 10^{-3}/ year and 10^{-6}/ year. In general, there is a multiplicative factor of 10 or 100 between the two values.

We prefer this ALARP approach instead of the renunciation issued from the precautionary principle. Normally this principle should be an incitement to break the uncertainty (by operation feedback, by research, by physical tests...). In reality it leads very often to a renunciation of action including in particular innovative projects. This ALARP approach is mainly used in the frame of process industries or extreme natural aggressions.

Another approach called GALE (Globally At Least Equivalent) is used in the transport, particularly in the railway transportation. A new system or subsystem shall be designed, carried out or modified in such a way that the overall level of safety after its modification is at least equivalent to that resulting from the implementation of existing systems or subsystems providing comparable services or functions.

Any risk analysis requires a probabilistic quantification, which is always possible in the uncertainty domain of Medianistan (note that Taleb uses Mediocristan (no observed event can have a significant impact on the whole), but we think that Medianistan introduced by [LEM 14] is a more adapted word), in the domain of the median or of the mean [TAL 10]. Results have to be examined in relative. Beware of only qualitative analysis, always necessary but insufficient and often not objective. When estimating the probability is difficult or when a plausible event is very unlikely, which characterizes the uncertainty domain of Extremistan (*the black swan,* a single observed event can have a great impact on the whole), it becomes very important to consider the physical models to calculate the consequences; are these consequences acceptable? The consequences assessment is the first step, the first parade to protect against unforeseen events.

The probabilistic approach should be practiced. It is a good indicator of the safety / security of a socio-technical system or process. Even if often it is only relative to the functional and physical aspects, it may implicitly reflect the weaknesses of human behavior and organizational factors. A quantitative presentation is always useful because it allows to understand risks, to prioritize them, to guide and to complete expert analysis, to identify the critical points, to base the decisions taken.

Risk management is a continuous process that should be reviewed regularly to ensure that preventive and protection mechanisms in place meet the required objectives.

In the 2010s, the public feels a deep aversion to risk, he wants a zero risk and still be protected. Curiously there is at the present time a return to qualitative risk analysis methods. While the qualitative analysis is essential, it precedes quantitative analysis, but it is not sufficient, it is not objective. Be limited to qualitative analysis can only lead to sub-safety or cost overruns. This return to qualitative analysis could also be attributed to the aversion of decision makers to probabilistic approaches.

Safety studies revert priorities and move towards major public concerns: the impact of extreme natural events, probability of rare events, estimation of consequences, costs of safety, emerging risks, risks related to climate change, terrorism, risks related to innovative products, ...

6.2. *Help for decision making*

In early 1990s, the decision tree and the cost - benefit analysis were the methods used by engineers. They are particularly welcome when the decision has to be economical. And they are still widely used in 2015.

Risk analysis is frequently used to demonstrate the conformity of an industrial site to the requirements of regulation rules. Nevertheless, quantitative risk analysis can be considered as an important input of decision making. The task of the decision maker is very difficult in the sense that his/her decision can lead to negative consequences. Generally, he has to choose one action (or option) among many, every one leading to uncertain consequences, more or less serious.

First of all, he will listen to the analyst, looking at the risk assessment results and their uncertainties, their robustness, the sensitivity analysis, the models used, the uncertainties concerning input data including quality of feedback and reliability of expertise, social, economical and environmental stakes.

Since most actions may have uncertain negative consequences, considering the industry stakes, the decision maker must specify his preferences which can concern for instance:

– in the RCM frame: safety, availability, maintenance costs [BEA 99],

– or in the frame of design phase: availability, investment and delay…

These parameters are called attributes and the decision maker has to give a hierarchy of these attributes determining his degree of preferences. It is important that these attributes can be measured, even subjectively, or in using indicators which are representative and measurable. A utility function can be elicited taking into account the risk attitude of the decision maker [BEA 09].

In practice, in 2015, the decision maker is faced with several objectives (safety, industrial performance, costs, ...) and must choose between several options in a very uncertain environment. The Multi-Attribute Utility Theory (MAUT) methods help him in his decision and therefore are increasingly used [EDW 07; BEA 14].

Main popular decision analysis methods are listed in the table 6.2 hereunder (see also [BED 04]). Note also an increasing use of asset management models especially when it comes to optimize the life extension of an industrial plant or its durability (preventive maintenance, predictive maintenance) and of Bayesian networks when measuring the effectiveness of an action or option has to be assessed.

Method	Where is used the method?	Use of expertise	Some characteristics
Cost-benefit analysis	Risk analysis	Probabilities, seriousness of potential accidents Costs of safety	Basis for a consensus decision
Decision tree	Reliability and corrective / preventive maintenance Design phase	Assessment of reliability parameters	Finite number of actions Economical utility
Making decision using Bayesian inference	Reliability, PSA, maintenance, durability Treatment of modifications	Updating of data Effects of modifications	After definition of a mitigation action (or option)
Electre methods	Risk analysis Environmental risks Durability	Elicitation of preferential information, outranking methods and aggregation	Multiple criteria approach, based on the concept of relationship, accepts a share of incomparability
MAUT, multi attribute utility theory	Risk analysis when rare events (small probabilities, major consequences) Safety, maintenance optimization, help for new design	Elicitation of preferences, of a utility function	Decision under uncertainty Action studied a priori defined Attributes measurable
LCM, Life Cycle Management	Risk informed asset management. Optimization of maintenance Life extension	Screening Definition of actions (options) Assessment of reliability parameters	Optimization of the NPV (*net present value*) Asset management models
Belief networks	Risk analysis Diagnosis, prognosis, optimization of maintenance Proactive behavior	Construction of the belief net Probabilities of the nodes, conditional probabilities Verification- validation of the model	Qualitative and quantitative variables Takes into account uncertainties Permits to think of new actions
Influence diagrams	Organizational and management factors Maintenance Human factor probabilities	Influent factors Qualitative influence Conditional probabilities	Conditional independence

Table 6.2. *Main decision analysis methods used in risk management, safety and dependability [LAN 14; MER 10].*

7. Conclusion: and now, which future?

This article is a quick overview of some topics of risk management and dependability from 1990 to 2015. It reflects the views observed by the author on these 25 years.

Risk management and dependability are approaches that respond to a system behavior and deal with uncertainty. They consider all factors that may affect the performance and they provide a quantitative

assessment. They predict the ability to perform required functions and explore consequences when they do not. The utilizations of risk management and dependability have also the following characteristics: they are important methods and tools to aid managers in decision making, they can compare alternative options, they are cost-efficient, they are widely used in Europe, they remain an active R&D area around Europe.

Risk management requires a quantitative approach, deterministic and probabilistic. Real life is uncertain, it is probabilistic. The risk analysis which is limited to a qualitative analysis is doomed to failure.

Understanding the past prepares the future. Risk management and dependability appear with a promising future. Table 7 summarizes the study subjects, considered priority by the author, which could be conducted in the near future. The last column of this table offers some basic references for further work.

Topics		List of subjects for the near future	Basic references for further work
Modeling and propagating uncertainty	Dependability methods, system analysis at the design phase	Dependability of innovative products Modeling complexity Improvement of knowledge, management of knowledge Dynamic reliability Organizational and human factors in the design Impact on health and environment	[VIL 88] [COC 97] [BOU 08] [BAT 16]
	Structural safety	Industrial applications Processing of data Reliability and robustness Time variant reliability Practical guide	[DIT 96] [ROC 08] [LEM 14]
	Maintenance modeling	Maintenance optimized Efficiency of maintenance Failure diagnosis and prognosis, HUMS	[COR 06] EN13306: 2010 [DOY 11] [PRO 11]
	Ageing management	Analysis of degradations Predictive maintenance Diagnosis, prognosis Asset management models Ageing management data basis	[NIK 02] [LAN 05] [USNRD 10] ISO 55000: 2014
	Influence diagrams and belief networks	Belief networks: benefits and difficulties Industrial applications Application to human and organizational factors	[JEN 96] [SIM 12]
Collecting, validating and analyzing uncertain data	Operation feedback: failures and degradations	Big data Automatic treatment of language Text mining HUMS systems Knowledge management	[LAN 94] [IMdR 15] [MER 16]
	Frequentist methods and Bayesian inference	Fusion of heterogeneous data Practical guide	[MEE 98] [SIN 06]
	Operation feedback: accident analysis	Weak signals Probability of rare events Consequences models International data basis on major events	[ESReDA 09] [DEH 13] [JOU 14] [GER 16]
	Expert opinion	Elicitation, bias, uncertainties, trust in expertise Fuzzy logic Use of expertise: knowledge management	[COO 91] [COJ 98] [BOL 05]
	Human factor data	Methods for quantifying human and organizational factors Text mining	[SWA 83] [EMB 92]

		International data basis on events and simulator experience to support quantification	[LEB 10] [AGU 13] [BLA 14]
Deciding in an uncertain context	Risk analysis, safety, accepting risk	Methods, techniques and tools for risk analysis; balance between safety and profitability Safety indicators Efficiency of barriers Acceptance criteria	ISO 31000-31010: 2009 [AVE 10] [TAL 10] [KER 10]
	Help for decision making	Development and use of MAUT methods Risk informed asset management Practical guide	[BEA 09] [MER 10] [LON 12]

Table 7. *Priority topics to be developed in the near future*

Acknowledgements

The author thanks strongly the University Blaise Pascal in Clermont-Ferrand and Professor Alaa Chateauneuf for their invitation to present this paper at the 51st ESReDA seminar. The author warmly thanks Maurice Lemaire, Professor Emeritus at the IFMA (French Institute of Advanced Mechanics, Clermont-Ferrand) for his review and his relevant comments.

Bibliography

[AGR 13] AGUIRRE F., SALLAK M., SCHÖN W., BELMONTE F. (2013), Application of evidential networks in quantitative analysis of rail way accidents, Proceedings of the Institute of Mechanical Engineers, *Journal of Risk and Reliability*, Vol 227, N° 4, pp 368-384, November 2013.

[AND 02] ANDREWS J. and MOSS T.R. (2002), *Reliability and Risk Assessment*, PEPL, Bury.

[AND 10] ANDREWS J., BERENGUER C., JACKSON L. editors (2010), *Maintenance Modeling and Applications*, An ESReDA project group report, Det Norske Veritas.

[ANR 04] ANDRIEU-RENAUD C., SUDRET B., LEMAIRE M. (2004), The PHI2 method: a way to compute time-variant reliability, *Reliability Engineering and System Safety*, Vol 84, Issue 1, pp 75-86, April 2004.

[ARD 10] ARDILLON E. editor (2010), SRA into SRA: Structural Reliability Analyses into System Risk Assessment, An ESReDA project group report, Det Norske Veritas.

[ARIA] ARIA, Retour d'expérience accidents technologiques, www.aria.developpement-durable.gouv.fr

[AVE 10] AVEN Terje (2010), *Misconceptions of Risk*, Wiley, 2010.

[BAC 98] BACHA M., CELEUX G., IDEE E., LANNOY A., VASSEUR D.(1998), *Estimation de modèles de durées de vie fortement censurées*, collection de la direction des études et recherches d'Electricité de France, Eyrolles, 99.

[BAI 13] BAILLIF L., PLANCHETTE G. (2013), *Sensibilisation aux concepts cindyniques*, AFNOR, MAR-A-I-30-60, avril 2013.

[BAR 65] BARLOW R.E., PROSHAN F. (1965), *Mathematical Theory of Reliability*, John Wiley&Sons, Inc. New York.

[BAR 93] BARLOW R., CLAROTTI C., SPIZZICHINO F. (editors) (1993), *Reliability and decision making*, Chapman & Hall.

[BAT 16] BATTEUX M., PROSVIRNOVA T., RAUZY A. (2016), A reasoned introduction to Model-Based Risk and Safety Assessments, tutorial A3, λμ20 Conference, Saint-Malo, October 2016.

[BAY] Bayesia software, www.bayesia.com

[BEA 99] BEAUDOUIN F., MUNIER B., SERQUIN Y. (1999), Multi-attribute decision making and generalized expected utility in nuclear power plant maintenance, in *Interactions and Preferences in Decision Making*, Kluwer Academic Publishers, New York, pp 341-357.

[BEA 09] BEAUDOUIN F., MUNIER B. (2009), A revision of industrial risk management, *Risk and Decision Analysis*, vol 1, pp 3-20.

[BEA 14] BEAUDOUIN F., MEUWISSE C. (2014), *Classement de tours aéroréfrigérantes en fonction du risque global de ruine – Développement et mise en œuvre d'un système d'aide à la décision*, Proceedings of the JFMS, Aix-en-Provence, 09-10 April 1994.

[BED 01] BEDFORD T., COOKE R. (2001), *Probabilistic Risk Analysis-Foundations and Methods*, Cambridge University Press.

[BED 04] BEDFORD T., CHRISTENSEN P., PROCACCIA H. editors (2004), *Decision Analysis for Reliability Assessment*, An ESReDA project group report, Det Norske Veritas.

[BEN 09] BENAVOLI A B. RISTIC, A. FARINA, M. OXEHAM, L. CHISCI (2009), An application of evidential networks to threat assessment, Aerospace and Electronic Systems, *IEEE Transactions*, Vol 45, n°2, pp 620-639.

[BIC 08] BICKING F., SIMON C., AUBRY J-F (2008), *Aide à la conception de systèmes instrumentés de sécurité*, Congrès λμ16, 6-10 octobre 2008, Avignon.

[BIE 98] BIEDER C., LE BOT P., DESMARES E., BONNET J-L. CARA F. (1998), MERMOS, *EDF's new advanced Human Reliability Analysis method*, PSAM4, A. Mosleh and R.A. Bari editors, Springer Verlag, New York.

[BLA 14] BLATTER C., RAYNAL C. (2014), *Textual analysis methods to interpret human, organizational and technical safety reports*, λμ19 Conference, Dijon, October 2014.

[BOL 05] BOLADI -LAVIN R., DEVICTOR N. (2005), CEA-JRC Workshop « the use of expert judgment in decision making », Aix-en-Provence, 21-23 June 2005.

[BOU 97] BOUISSOU M., BOURGADE E. (1997), *Unavailability evaluation, and allocation at the design stage for electric power plants: methods and tools*, RAMS' 97, Philadelphie, January 1997.

[BOU 08] BOUISSOU, M. (2008) *Gestion de la complexité dans les études quantitatives de sûreté de fonctionnement de systèmes*, Lavoisier, Editions Tec&Doc.

[BOUR 98] BOURGADE E., DEGRAVE C., LANNOY A. (1998), Performance improvements for electrical power plants: designing in the context of availability, ESREL'1998, in *Probabilistic Safety Assessment*, Cacciabue C., Papazoglou I.A. Editors, Springer and Verlag, Heidelberg, pp 158-162.

[BOUZ 05] BOUZAÏENE-MARLE Leïla, (2005), AVISE, anticipation des défaillances potentielles dues au vieillissement par analyse du retour d'expérience, thesis of Ecole Centrale Paris.

[CAM 08] CAMBON J., GUARNIERI F. (2008), *Maîtriser les défaillances des organisations en santé et sécurité au travail : la méthode TRIPOD*, Editions Lavoisier, Collection Sciences du Risque et du Danger.

[CCPS 89] CCPS, Center for Chemical Process Safety (1989), *Guidelines for Process Equipment Reliability Data with Data Tables*, American Institute of Chemical Engineers, New York.

[CEN 02] CEN (2002), *Eurocode: Basis of Structural Design*, EN 1990, December 2002.

[CHA 17]CHATEAUNEUF A. editor (to be published in 2017), *Reliability-based Life Cycle Cost Optimization of Structures and Infrastructures*, An ESReDA project group report.

[CLA 93] CLAROTTI C.A. (1993), Inevitability of the Bayesian Predictive Approach to PRA's, in *Safety and Reliability Assessment- an Integral Approach*, P. Kafka and J. Wolf Eds, Amsterdam, Elsevier, pp 885-899.

[CLA 94] CLAROTTI C, LANNOY A, PROCACCIA H, VILLAIN B. (1994). *ARCS : outil logiciel pour la quantification de l'effet de la maintenance sur la durée de vie*, λμ 9 Conference, ESREL'94, La Baule.

[CLA 98] CLAROTTI C. A. (1998), *Les techniques fréquentielles et bayésiennes au service de l'ingénieur de sûreté de fonctionnement*, Les projets de l'ISdF, Paris, www.imdr.eu.

[CLA 04] CLAROTTI C., LANNOY A., ODIN S., PROCACCIA H. (2004), Detection of equipment aging and determination of the efficiency of a corrective measure, *Reliability Engineering and System Safety*, Volume 84, Issue 1, Avril 2004, 57-64.

[COC 97] COCOZZA-THIVENT Christiane (1997), *Processus stochastiques et fiabilité des systèmes*, Springer.

[COJ 98] COJAZZI G., GUIDA G., PINOLA L. (1998), in A. Mosleh, R.A Bari (Eds), *Expert Judgement Methodology and its Application in the Prediction of the Results of a Fuel Coolant Interaction Experiment*, PSAM4, 13-18/09/1998, New-York City, Springer-Verlag, London.

[COJ 01] COJAZZI G., et al. (2001) Benchmark Exercise on Expert Judgment Techniques in PSA level 2., *Nuclear Engineering & Design*, vol. 209, pp. 211-221.

[CON 06] CONDAMIN Laurent, LOUISOT Jean-Paul, NAÏM Patrick (2006), *Risk Quantification (Management, Diagnosis and Hedging)*, John Wiley & Sons Limited.

[COO 91] COOKE R.MR (1991), Experts in Uncertainty, Expert Opinion and Subjective Probability in Science, Oxford University Press; New-York, 1991.

[COR 06] CORSET F., CELEUX G., LANNOY A., RICARD B. (2006), Designing a bayesian network for preventive maintenance from expert opinions in a rapide and reliable way, *Reliability Engineering and System Safety*, Vol 91/7, 849-856.

[COS 10] COSTA, O.L.V., DUFOUR F. (2010), Average Continuous Control of Piecewise Deterministic Markov Processes, *SIAM Journal on Control and Optimization*, 48 (7).

DAKOTA, www.dakotasoft.com/solutions, open source software.

[DAV 84] DAVIS M.H.A. (1984), Piecewise Deterministic Markov Processes – A General Class of Non Diffusion Stochastic Models, *Journal of The Royal Statistical Society*, Series B (Methodological), 46(3), pp 353-388.

[DEH 13] DEHEUVELS Paul (2013), Evénements rares et risques extrêmes, Invited lecture at the Qualita 2013 Conference, Technological University of Compiègne, http://www.utc.fr/fim/fc/video/watch/id/1298/

[DEHP 04] DEHOMBREUX P., HOU G., BASILE O., RIANE F. (2004), *Integration of condition monitoring in a reliability based maintenance policy*, 26th ESReDA seminar « lifetime management of industrial systems", Tampere, Finland.

[DEL] DELAGE A., LANNOY A., LEMAIRE M. et al (to be published), *Fiabilité en mécanique : des méthodes aux applications.*

[DER 08] DE ROCQUIGNY E., DEVICTOR, N., TARANTOLA, S. et al (2008), *Uncertainty in Industrial Practice – A guide to quantitative uncertainty management*, Wiley.

[DERK 09] DER KIUREGHAN A., DITLEVSEN O. (2009), Aleatoty or epistemic ? Does it matter?, *Structural Safety*, vol 31, pp 105- 112.

[DIT 96] DITLEVSEN O., MADSEN H. (1996), *Structural Reliability Methods*, John Wiley & Sons, New York.

[DOY 11] DOYEN L., GAUDOIN O. (2011), Modelling and assessment of ageing and efficiency of corrective and planned preventive maintenance actions, *IEEE Transactions on Reliability*, 2011: 60(4): 759-69.

[DUB 11] DUBOURG V., SUDRET B., BOURINET J-M. (2011), Reliability based design optimization, using kriging surrogates and subset simulation, *Structural and Multidisciplinary Optimization*, vol 44, n°5, pp 673-690.

[DUF 02] DUFOUR F., DUTUIT Y. (2002), *Dynamic reliability – A new model*, Proceedings of ESREL'2002 – λμ 13 Conference, Lyon, pp 350-353.

[EDW 07] EDWARDS E., MILES R., VON WINTERFELD D. et al (2007), *Advances in Decision Analysis: from Foundations to Applications,* Cambridge University Press.

EIReDA (1998, 2000), see to Procaccia et al.

[EMB 92] EMBREY, D.E. (1992), Incorporating management and organisational factors into probabilistic safety assessment, *Reliability Engineering and System Safety*, 38, 199-208.

EN 13306: 2010, *Maintenance terminology*, 2nd edition, October 2010

EN 62251: 2012, *Analysis Techniques for Dependability – Petri Net Techniques*, November 2012.

[EPRI 93] EPRI, Electric Power Research Institute (1993), *Common Aging Methodology*, february 1993.

[ESReDA 09] ESReDA project group on Accident Investigation (2009), *Guidelines for Safety Investigations of Accidents*, www.esreda.org.

FERUM, www.ce.berkeley.edu/projects/ferum, open source software.

[FIDES 09] FIDES (2009), UTE-C 80-811 (Janvier 2011) Guide FIDES 2009 - Edition A – September 2010: *Méthodologie de fiabilité pour les systèmes électroniques*.

[FIS 78] FISCHOFF B., SLOVIC P., LICHTENSTEIN S., READ S., COMBS B. (1978), *How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits*, Policy Sciences 9, pp 127-152, Elsevier.

[FOR 09] FORESTER J. A., COOPER S.E., LOIS E., KOLACZKOWSKI A.M., BELEY D.C., WREATHALL J. (2009), *An overview of the evolution of Human Reliability Analysis into the context of Probabilistic Risk Assessment*, Sandia Report SAND2008-5085.

[GAO 96] GAO Yingzhong (1996), Modèles probabilistes et possibilistes pour la prise en compte de l'incertain dans la sécurité des structures, Thèse ENPC, 02 May 1996.

[GER 05] GERTMAN D., BLACKMAN H., MARBLE J., BYERS J., SMITH C. (2005), *The SPAR-Human Reliability Analysis Method,* NUREG/CR-6883, US NRC.

[GERV 16] GERVILLE-REACHE L., COUALLIER V., BAYLE F. (2016), *Approches comparées sur l'estimation d'une probabilité de défaillance: cas des échantillons totalement censurés*, Journée IMdR « Estimation de probabilités d'évènements rares », ESTP Cachan, 09 June 2016.

GRIF (update 2016.15),software platform for determining the essential indicators of dependability, www.grif-workshop.com .

[HAS 74] HASOFER A.M., LIND N.C. (1974), Exact and invariant second moment code format, *J. Eng. Mech*., Div. Proc. ASCE 100 (EM1), pp 101-121.

[HIL75] Hill B. M. (1975), A Simple General Approach to Inference about the Tail of a Distribution, *The Annals of Statistics*, 3, pp 1163-1174.

[HOL 98] HOLLNAGEL G. (1998), *Cognitive Reliability and Error Analysis Method*, Elsevier, Amsterdam.

[HOUR 14] HOURTOLOU D., SALVI O. (2014), Aramis project: accidental risk assessment methodology for industries in the framework of Seveso II directive, http://hal.ineris.ccsd.inrs.fr/ineris-00972444

[HSE 92] HSE (1988). Health and Safety Executive: *The Tolerability of Risk from Nuclear Power Stations*. Discussion Document, HMSO, London. Revised edition, 1992.

[IAEA 02] IAEA (2002), *Guidance on effective management of the physical ageing of systems, structures and components important to safety for nuclear power plants*, version 1, Vienna.

[IAEA 08] IAEA (2008), *Collection and classification of human reliability data for use in probabilistic safety assessments,* Vienna.

IEC 61165: 2006, *Application of Markov techniques*, edition 2.0.

IEC 61508: 2010 (2010), *Functional safety of electrical/ electronic / programmable electronic safety- related systems*.

[IMdR 15] IMdR (2015), Project P15-2, HUMS/ Health and Usage Monitoring System, project manager: Michel Giraudeau, November 2015.

[INPO 01] INPO (2001), *Equipment Reliability Process Description*, November 2001.

ISO 14224: 2016 (2016), *Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment,* Third edition.

ISO 31000: 2009 (2009), *Risk management – principles and guidelines* (see also ISO/ TEC 31010 (2009) – *Risk management-risk assessment techniques)*.

ISO 55000: 2014 (2014), series of *Asset Management standards*, January 2014.

[JEN 96] JENSEN F.V. (1996), *An introduction to Bayesian Networks*, UCL Press(Ed), London.

[JOH 74] JOHNSON L. (reprint 1974), *The statistical treatment of fatigue experiments*, Elsevier.

[JOU 14] JOUNIAUX P., HADIDA D., DECHY N., MARLE L. (2014), *Detection, relevance and amplification of weak signals within the learning of experience*, λμ19 Conference, Dijon, October 2014.

[KAH 10] KAHN, P., LANNOY, A., PERSON-SILHOL and VASSEUR, D. (2010), *Anticipation, innovation, perception – Des défis pour la maîtrise des risques à l'horizon 2020*, Lavoisier, Editions Tec&Doc.

[KAP 58] KAPLAN E.L. and MEIER P., (1958), Non parametric estimation from incomplete observations, *Journal of the American Statistical Association*, 53, 457-481.

[KER 10] KERMISCH Céline (2010), *Les paradigmes de la perception du risque*, Lavoisier, Tec&Doc

[KERV 91] KERVERN G.-Y., RUBISE P. (1991), *L'archipel du danger – Introduction aux cindyniques*, Economica, Paris ; (1994) *Latest advances in cindynics*, Economica.

[KLE 82] KLEFSJÖ Bengt (1982), On aging properties and Total Time on Test transforms, *Scand. J. Statis*. 9: 37-41, 1982.

[LAN 94] LANNOY A., PROCACCIA H. (1994) *Méthodes avancées de traitement et d'analyse de banques de données du retour d'expérience*. Collection de la Direction des Etudes et Recherches d'Electricité de France, Editions Eyrolles N° 86, Paris.

[LAN 01] LANNOY A., PROCACCIA H. (2001), *L'utilisation du jugement d'expert en sûreté de fonctionnement*, Lavoisier, Editions Tec&Doc.

[LAN 04] LANNOY A. editor (2004), *Lifetime management of structures*, An ESReDA working group report, Det Norske Veritas, Høvik.

[LAN 05] LANNOY A., PROCACCIA H. (2005), *Evaluation et maîtrise du vieillissement industriel*, Lavoisier, Editions Tec&Doc.

[LAN 14] LANNOY A., PROCACCIA H. (2014), Expertise, safety, reliability, and decision making: practical industrial experience, *Environment Systems & Decisions*, Volume 34 Number 2: 259-276, June 2014, Springer.

[LAN 15] LANNOY A. (2015), Limites, insuffisances et apports des approches probabilistes actuelles : quelles leçons tirer ? Les Entretiens du Risque 2015, Maisons-Alfort, 03-04 November 2015, in *Risques Majeurs, incertitudes et décisions – Approche pluridisciplinaire et multisectorielle* (Merad et al, 2016), MA éditions.

[LEB 10] LE BOT P. (2010), Overview of the MERMOS Human Reliability Analysis Method, Idaho Falls, 11 August 2010, https://secure.inl.gov/isrcs2010/docs/abstracts/LeBot_MERMOS.pdf

[LEM 05] LEMAIRE Maurice (2005). *Fiabilité des structures, couplage mécano – fiabiliste statique*, in collaboration with Alaa CHATEAUNEUF and Jean-Claude MITTEAU, Hermès Lavoisier.

[LEM 14] LEMAIRE, M. (2014) *Mechanics and Uncertainty*, iSTE/ Wiley, Mechanical Engineering and Solid Mechanics Series.

[LI 06] LI Hong-shuong, LÜ Zhen-Zhou, YUE Zhu-feng (2006), Support Vector Machine for structural reliability analysis, *Applied Mathematics and Mechanics*, 2006, 27(10): 1295-1303.

[LIG 74] LIGERON J-C, MARCOVICI C. (1974), *Utilisation des techniques de fiabilité en mécanique*, Technique&Documentation, Paris.

[LON 12] LONCHAMPT J., FESSART K. (2012), *Investments Portfolio Optimal Planning for Industrial Assets Management – Method and Tool*, IAEA-CN-194-007.

[MAD 86] MADSEN H.O., KRENK S., LIND N.C. (1986), *Methods of Structural Safety*, Prentise-Hall.

[MAR 07] MARSEGUERRA M., ZIO E., LIBRIZZI M. (2007), Human Reliability Analysis by Fuzzy CREAM, *Risk Analysis,* vol 27, pp137-154.

[MEE 98] MEEKER W., ESCOBAR L. (1998), *Statistical methods for reliability data*, Wiley.

[MER 10] MERAD Myriam (2010), *Aide à la décision et expertise en gestion des risques*, Lavoisier, Editions Tec&Doc.

[MER 16] MERAD Myriam, DECHY Nicolas, DEHOUCK Laurent, LASSAGNE Marc, editors (2016), *Risques majeurs, incertitudes et décisions – Approche pluridisciplinaire et multisectorielle*, MA Editions-ESKA 2016.

[MERC 16] MERCIER-LAURENT Eunika (2016), *Connaissance et maîtrise des risques*, Article AFNOR III-50-31, march 2016.

MIL-STD-2173(1986), *Reliability-Centered Maintenance – Requirements for Naval Aircraft, Weapons Systems and Support Equipment*.

[MOR 15] MORIO Jérôme, BALESDENT Mathieu (2015), *Estimation of Rare Event Probabilities in Complex Aerospace and Other Systems – A Practical Approach*, Woodhead Publishing, Elsevier.

[MOS 05] MOSS T.R. (2005), *The Reliability Data Handbook*, Professional Engineering Publishing.

Netica software, Norsys Software Corp., www.netica.com/netica

[NIK 02] NIKULIN M., BAGDONAVICIUS V. (2002), *Accelerated life and degradation models in reliability and safety: an engineering perspective*, Chapman & Hall CRC,94.

OpenTURNS software, 1.6 released, august 2015, www.openturns.org

OREDA, *Offshore Reliability Data Handbook* (2015) - 6th edition, https://www.dnvgl.com/oilgas/publications/handbooks.html

[PET 99] PETTERSSON L. editor (1999), *Handbook on Quality of Reliability Data*, Det Norske Veritas.

[PET 01] PETTERSSON L. editor (2001), *Handbook on Maintenance Management*, Det Norske Veritas.

[PET 06] PETTERSSON L., SIMOLA K. editors (2006), *Ageing of Components and Systems*, An ESReDA working group report, Det Norske Veritas, Høvik.

[PRO 98] PROCACCIA H., ARSENIS S.P. and AUFORT P., Preface by VOLTA, G. (1998) *European industry reliability data bank EIReDA 1998*. EDF/ CEE JRC Ispra; *EIReDA'2000*, Crete University Press, Heraklion.

[PRO 09] PROCACCIA Henri (2009), *Introduction à l'analyse probabiliste des risques*, Collection Sciences du risque et du danger, Editions Tec&Doc, Lavoisier.

[PRO 11] PROCACCIA H., FERTON E., PROCACCIA M., (2011), *Vieillissement et maintenance des matériels et systèmes industriels réparables*, Lavoisier, Editions Tec&Doc.

[RAS 97] RASSMUSSEN Jens (1997), Risk management in a dynamic society: a modelling problem, *Safety Science* 27 (2-3), pp183-213.

[RAU 97] RAUZY A., DUTUIT Y. and SIGNORET J.-P. (1997), Monte-Carlo Simulation to Propagate Uncertainties in Fault Trees encoded by means of Binary Decision Diagrams in *Proceedings of the 1st International Conference on Mathematical Methods in Reliability*, MMR'97. pp 305–312.

[RAZ 14] RAZA M. editor (2014), *Reliability and Maintainability Impact to Asset Management Stakeholders*, An ESReDA project group report, Det Norske Veritas.

[REA 97] REASON J. (1997), *Managing the risks of organizational accidents*, Ashgate Publishing Ltd.

RiskSpectrum software, Lloyd's Register Consulting, www.riskspectrum.com.

[SAE 12] JA1000/1 (2012), *Reliability Program Standard Implementation Guide*, May 2012.

[SAL 06] SALLAK M., AUBRY J-F, SIMON C. (2006), Aide à la décision dans la réduction de l'incertitude des SIL: une approche floue possibiliste, https://hal.archives-ouvertes.fr/hal-00118741.

[SAN 03] SANDTORV Helge, OSTEBO Runar, KORTNER Henrik (2003), *Collection of reliability and maintenance data – development of an international standard*, ESREL'2005, Gdansk, Polen, A.A. Balkema Publishers.

[SCH 15] SCHINDLER J., WIEDMANN-SCHMIDT W. (2015), Im roten Bereich, *Der Spiegel* 10/ 2015, http://www.spiegel.de/spiegel/print/d-132040367.html

[SIG 14] SIGNORET J.-P. (2014), *Les réseaux de Petri: outils de modélisation et de calcul en sûreté de fonctionnement*, www.afnor.org, MAR-A-III-10-83, July 2014.

[SIM 99] SIMOLA Kaisa (1999), *Reliability methods in nuclear power plant ageing management*, VTT Publications 379, Espoo.

[SIN 97] SINGPURWALLA, N. (1997) Gamma processes and their generalizations: an overview. In: Cooke, R., et al. (eds.) *Engineering probabilistic design and maintenance for flood protection*, Kluwer Academic Publishers, pp. 67-73.

[SIN 06] SINGPURWALLA N. (2006), *Reliability and Risk – A Bayesian Perspective*, John Wiley & Sons, Ltd, Chichester.

[SLI 03] SLITER George, (2003), *Life cycle management in the US nuclear power industry*, SMIRT 17, Prague, 17-22 august.

[SOB 15] SOBRAL J., SERRANO E., FERREIRA L. (2015), *Methods, Techniques and Tools to Understand Human Error in Industrial Activities: a Review*, 49th ESReDA seminar, October 2015.

[SWA 83] SWAIN A.D., GUTTMANN H.E., 1983, *Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278, Washington, D.C., US Nuclear Regulatory Commission.

[TAL 10] TALEB N. N. (2010), *The Black Swan - The Impact of Highly Improbable*, The Random House Publishing Group, Second edition.

[TAL 13] TALEB N. N. (2013) *Antifragile, Things that Gain from Disorder*, Penguin.

T- Book (2005), *Reliability data of components in Nordic nuclear power plants*. 6th. ed, Swedpower AB, Stockholm (Sweden).

[THO 98] THOFT-CHRISTENSEN P. editor (1998), *Industrial Application of Structural Reliability*, ESReDA Safety Series No. 2, Det Norske Veritas, Høvik.

[USNRC 75] US NRC (1975), *Reactor Safety Study: an Assessment of Accident Risks in US Commercial Nuclear Power Plants*, WASH-1400, NUREG675/014, 1975.

[USNRC 83] US NRC (1983), *PRA Procedures Guide*, NUREG/CR-2300, 1983.

[USNRC 07] US NRC (2007), *Expert Panel Report on Proactive Materials Degradation Assessment*, NUREG/CR-6923, February 2007.

[USNRC 10] US NRC (2010), *Generic Aging Lessons Learnt (GALL) Report*, NUREG-1801 Revision 2.

[VIL 1988] VILLEMEUR A. (1988), *Sûreté de fonctionnement des systèmes industriels*, collection de la direction des études et recherches d'Electricité de France, 67, Eyrolles.

[WEB 12] WEBER P., MEDINA-OLIVIA G., SIMON C., IUNG B. (2012), Overview on Bayesian Networks – Applications for Dependability, Risk Analysis and Maintenance Areas, *Engineering Applications of Artificial Intelligence*, 25,4, June, pp 671-682.

[WEL 74] WELKER Every, LIPOW Myron (1974), *Estimating the Exponential Failure Rate From Data with No Failures*, Proceedings of the 1974 Annual Reliability and Maintainability Symposium, Los Angeles, California, page 420 – 427, IEEE Catalog Number 74CHO820-1RQC, Volume 7, Number 2, Institute of Electrical and Electronics Engineers, New York, New York, 1974.